PCT/JP99/05689

14.10.99

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

EKJ

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

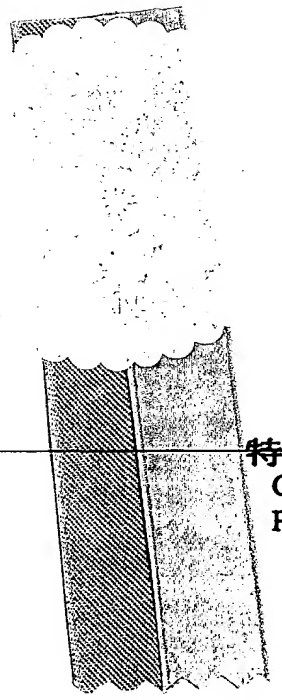
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年１０月１９日

出願番号
Application Number: 平成１０年特許願第２９６９４２号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a)OR(b)



１９９９年 ８月２４日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０５９１４４

【書類名】　特許願

【整理番号】　9801034108

【提出日】　平成10年10月19日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明の名称】　情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体

【請求項の数】　9

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北原　淳

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体

【特許請求の範囲】

【請求項１】　装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置において、

装着された前記外部記憶媒体と相互認証する相互認証手段と、

所定の鍵で所定の情報を暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記所定の鍵は、前記情報処理装置を管理する管理装置の公開鍵である

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、

装着された前記外部記憶媒体と相互認証する相互認証ステップと、

所定の鍵で所定の情報を暗号化する暗号化ステップと

を含むことを特徴とする情報処理方法。

【請求項４】　装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置に、

装着された前記外部記憶媒体と相互認証する相互認証ステップと、

所定の鍵で所定の情報を暗号化する暗号化ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項５】　暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段

を備えることを特徴とする管理装置。

【請求項６】　暗号化された情報を復号し、利用する情報処理装置を管理する管理方法において、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップ

を含むことを特徴とする管理方法。

【請求項７】　暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、

前記情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項８】　装着された外部記憶媒体に所定の情報を記憶させると共に、暗号化された情報を復号し、利用する情報処理装置、および前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記情報処理装置は、

装着された前記外部記憶媒体と相互認証する相互認証手段と、

前記管理装置の公開鍵で所定の情報を暗号化する暗号化手段と、

を備え、

前記管理装置は、

前記外部記憶媒体に記憶されたデータを復号する復号手段

を備えることを特徴とする情報利用システム。

【請求項９】　暗号化された情報を復号し、利用する情報処理装置に装着される外部記憶媒体において、

前記情報処理装置と相互認証する相互認証手段

を備えることを特徴とする外部記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、管理装置および方法、情報利用システム

、提供媒体、並びに外部記憶媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、管理装置および方法、情報利用システム、提供媒体、並びに外部記憶媒体に関する。

【０００２】

【従来の技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。この情報処理装置において、情報の復号に必要な鍵および課金情報など所定の情報は、外部からの不正アクセスを排除できる記憶部に記憶される。

【０００３】

【発明が解決しようとする課題】

しかし、新たな機器を利用する場合、情報の提供者と再度、契約を行う必要がある。また、何らかの原因で、外部からの不正アクセスを排除できる記憶部に記憶された情報が破壊された場合、ユーザには、契約しているにもかかわらず、情報が利用できず、情報提供者には、利用済みの情報に対する課金情報等が利用できなければ、決済が不可能になる等の問題が発生する。また、外部からの不正アクセスを排除できる記憶部に記憶される情報をそのまま外部に記憶したのでは、不正に対する安全性が低下する。

【０００４】

本発明はこのような状況に鑑みてなされたものであり、不正に対する安全性を保持したまま、必要な情報を外部に記憶できるようにすることを目的とする。

【０００５】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、装着された外部記憶媒体と相互認証する相互認証手段と、所定の鍵で所定の情報を暗号化する暗号化手段とを備えることを特徴とする。

【０００６】

請求項３に記載の情報処理方法は、装着された外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む

ことを特徴とする。

【０００７】

請求項４に記載の提供媒体は、情報処理装置に、装着された外部記憶媒体と相互認証する相互認証ステップと、所定の鍵で所定の情報を暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００８】

請求項５に記載の管理装置は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

【０００９】

請求項６に記載の管理方法は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含むことを特徴とする。

【００１０】

請求項７に記載の提供媒体は、管理装置に、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１１】

請求項８に記載の情報利用システムは、情報処理装置が、装着された外部記憶媒体と相互認証する相互認証手段と、管理装置の公開鍵で所定の情報を暗号化する暗号化手段とを備え、管理装置が、外部記憶媒体に記憶されたデータを復号する復号手段を備えることを特徴とする。

【００１２】

請求項９に記載の外部記憶媒体は、情報処理装置と相互認証する相互認証手段を備えることを特徴とする。

【００１３】

請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体においては、装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化する。

【００１４】

請求項５に記載の管理装置、請求項６に記載の管理方法、および請求項７に記載の提供媒体においては、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する。

【００１５】

請求項８に記載の情報利用システムにおいては、情報処理装置が、装着された外部記憶媒体と相互認証し、管理装置の公開鍵で所定の情報を暗号化し、管理装置が、外部記憶媒体に記憶されたデータを復号する。

【００１６】

請求項９に記載の外部記憶媒体においては、情報処理装置と相互認証する。

【００１７】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１８】

すなわち、請求項１に記載の情報処理装置は、装着された外部記憶媒体と相互認証する相互認証手段（例えば、図１０の相互認証モジュール７１）と、所定の鍵で所定の情報を暗号化する暗号化手段（例えば、図１０の暗号化ユニット９３）とを備えることを特徴とする。

【００１９】

請求項５に記載の管理装置は、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号する復号手段（例えば、図２のユーザ管理部１８）を備えることを特徴とする。

【００２０】

請求項８に記載の情報利用システムは、情報処理装置が、装着された外部記憶媒体と相互認証する相互認証手段（例えば、図１０の相互認証モジュール７１）

と、管理装置の公開鍵で所定の情報を暗号化する暗号化手段（例えば、図１０の暗号化ユニット９３）とを備え、管理装置が、外部記憶媒体に記憶されたデータを復号する復号手段（例えば、図２のユーザ管理部１８）を備えることを特徴とする。

【００２１】

請求項９に記載の外部記憶媒体は、情報処理装置と相互認証する相互認証手段（例えば、図１０の相互認証モジュール８１）を備えることを特徴とする。

【００２２】

図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ１は、コンテンツプロバイダ２、ユーザホームネットワーク５等に配送用鍵Ｋｄを送信し、ユーザホームネットワーク５から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ２およびサービスプロバイダ３への利益分配の処理を行う。

【００２３】

コンテンツプロバイダ２は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォータマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ３に送信する。

【００２４】

サービスプロバイダ３は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク４を介して、コンテンツプロバイダ２から供給されたコンテンツに価格を付して、ユーザホームネットワーク５に送信する。

【００２５】

ユーザホームネットワーク５は、サービスプロバイダ３から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金

処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク５が配送用鍵Ｋｄを EMDサービスセンタ１から入手する際、EMDサービスセンタ１に送信される。

【００２６】

図２は、EMDサービスセンタ１の機能の構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給するとともに、コンテンツプロバイダ２から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ３に配送用鍵Ｋｄを送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信するとともに、利益分配の情報を供給する。著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、コンテンツプロバイダ管理部１２、またはユーザ管理部１８等を介して、配送用鍵Ｋｄをコンテンツプロバイダ２、またはユーザホームネットワーク５等に供給する。ユーザ管理部１８は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部１５に記憶させる。

【００２７】

EMDサービスセンタ１からコンテンツプロバイダ２およびユーザホームネットワーク５を構成するレシーバ５１（図１０で後述する）への、配送用鍵Ｋｄの定期的な送信の例について、図３乃至図６を参照に説明する。図３は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５１がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００２８】

図３の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可

能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００２９】

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００３０】

また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用

できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００３１】

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３２】

１９９８年２月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図４で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００３３】

１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３４】

１９９８年３月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し

、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

【００３５】

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３６】

１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン４乃至バージョン６である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００３７】

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３８】

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザーが１，２ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【００３９】

利益分配部１６は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、EMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益を算出する。相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の所定の機器と後述する相互認証を実行する。

【００４０】

ユーザ管理部１８は、ユーザ登録データベースを有し、ユーザホームネットワーク５の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク５がEMDサービスセンタ１と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部１８は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク５の所定の機器に送信する。

【００４１】

図７に示すユーザ登録データベースの例は、ユーザホームネットワーク５の機器の機器固有の６４ビットからなるID（Identification Data）を記録し、そのIDに対応して（すなわち、そのIDを有する機器毎に）、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ１と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはサービスプロバイダ３などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部１８は、その登録を

拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【００４２】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク５が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である１台の機器は、EMDサービスセンタ１に、ユーザホームネットワーク５のEMDサービスセンタ１に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ１と接続が可能か否かの情報は、その機器が、EMDサービスセンタ１と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク５の他の機器を介して、EMDサービスセンタ１に、課金情報等を出力する。

【００４３】

また、ユーザ管理部１８は、ユーザホームネットワーク５の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部１５に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを供給する。

【００４４】

課金請求部１９は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【００４５】

図８は、コンテンツプロバイダ２の機能の構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付

加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマークを付加し、圧縮部３３に供給する。圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４６】

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをEMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４７】

DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００４８】

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００４９】

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回

繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００５０】

ポリシー記憶部３７は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部３８に出力する。セキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ２の公開鍵Ｋｐｃｐを含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ３に供給する。相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証し、また、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証する。

【００５１】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００５２】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００５３】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、

計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4，MD5，SHA-1などが用いられる。

【００５４】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００５５】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００５６】

次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d，e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００５７】

暗号文Cは、平文Mから、式（１）の処理で算出される。

C=M^e mod n　　(1)

【００５８】

暗号文Cは、式（２）の処理で平文Mに、復号される。

M=C^d mod n　　（２）

【００５９】

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるの

は、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

M=C^d=(M^e)^d=M^(ed) mod n　（３）

【００６０】

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００６１】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

C1=M+rnB　（４）

C2=rB　（５）

【００６２】

暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。

M=C1-nC2　（６）

【００６３】

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００６４】

図９は、サービスプロバイダ３の機能の構成を示すブロック図である。コンテンツサーバ４１は、コンテンツプロバイダ２から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部４４に供給する。値付け部４２は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ

作成部４４に供給する。ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部４４に供給する。相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証し、また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証する。また、コンテンツプロバイダ２が取扱方針を配送用鍵Ｋｄで暗号化して供給する場合、相互認証部４５は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受け付けるのに先立ち、EMDサービスセンタ１と相互認証する。

【００６５】

図１０は、ユーザホームネットワーク５の構成を示すブロック図である。レシーバ５１は、ネットワーク４を介して、サービスプロバイダ３からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【００６６】

通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)６２は、サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Ｋｄ等を記憶する。伸張部６３は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC（Integrated Circuit）カードインターフェース６４は、SAM６２からの信号を所定の形式に変更し、レシーバ５１に装着されたICカード５５に出力し、また、ICカード５５からの信号を所定の形式に変更し、SAM６２に出力する。

【００６７】

サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、課金処理を実行し、コンテンツ鍵Ｋｃｏを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM６２は、相互認証モジュール７１、課金モジュール７２、記憶モジュール７３、および復号／暗号化モジュール７４から構成さ

れる。このSAM６２は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【００６８】

相互認証モジュール７１は、サービスプロバイダ３、またはEMDサービスセンタ１との相互認証を実行し、必要に応じて、一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。課金処理モジュール７２は、サービスプロバイダ３から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール７３またはHDD(Hard Disk Drive)５２に出力する。記憶モジュール７３は、課金処理モジュール７２または復号／暗号化モジュール７４から供給された課金情報、および配送用鍵Ｋｄ等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Ｋｄ等のデータを供給する。

【００６９】

復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、所定の桁数の乱数を発生し、保存用鍵Ｋｓａｖｅとして暗号化ユニット９３および記憶モジュール７３に出力する。ただし、一度生成して保持している場合、その必要はない。暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に出力する。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６３に送信するとき、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。

【００７０】

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部６３は、相互認証モジュール７５、復号モジュール７６、復号モジュール７７、伸張モジュール７８、およびウォータマーク付加モジュール７９から構成される。相互

認証モジュール７５は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール７６に出力する。復号モジュール７６は、記憶モジュール７３から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール７７に出力する。復号モジュール７７は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール７８に出力する。伸張モジュール７８は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール７９に出力する。ウォータマーク付加モジュール７９は、コンテンツにレシーバ５１を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００７１】

HDD５２は、サービスプロバイダ３から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ３から供給されたコンテンツを記録し、再生するレコーダ５３は、記録再生部６５、SAM６６、および伸張部６７から構成される。記録再生部６５は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM６６は、SAM６２と同じ機能を有し、その説明は省略する。伸張部６７は、伸張部６３と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ５４は、装着された図示せぬMDにサービスプロバイダ３から供給されたコンテンツを記録し、再生する。

【００７２】

ICカード５５は、レシーバ５１に装着され、記憶モジュール７３に記憶された配送用鍵Ｋｄおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ５１を購入し、今まで使用していたレシーバ５１と入れ替えて使用する場合、まず、ユーザは、ICカード５５に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶されていた配送用鍵Ｋｄなどの所定のデータを記憶させる。次に、ユーザは、そのICカード５５を新たなレシーバ５１に装着し、そのレシーバ５１を操作して、EMDサービスセンタ１のユーザ管理部１８にその新たなレシーバ５１を登録する。EMDサービスセンタ１のユーザ管理部１８は、ICカード５５に記憶されていたデータ（今まで使用していたレシーバ５１のIDなど）を基

に、ユーザ管理部１８が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード５５は、相互認証モジュール８０および記憶モジュール８１で構成される。相互認証モジュール８０は、SAM６２と相互認証する。記憶モジュール８１は、ICカードインターフェース６４を介して、SAM６２から供給されたデータを記憶し、記憶したデータをSAM６２に出力する。

【００７３】

図１１は、ユーザホームネットワーク５の他の構成例を示すブロック図である。この構成のレシーバ５１およびレコーダ５３は、図１０に示した伸張部６３および伸張部６７を省略した構成を有する。その代わり、レコーダ５３に接続されているデコーダ５６が、伸張部６３または伸張部６７と同じ機能を有する。その他の構成は、図１０における場合と同様である。

【００７４】

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ５６は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２またはSAM６６と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、SAM６２から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにデコーダ５６を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００７５】

図１２は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバ

イダ３、およびユーザホームネットワーク５の間で送受信される情報を説明する図である。コンテンツプロバイダ２は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図１３を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ２の証明書（その詳細は図１４を参照して後述する）を付して、サービスプロバイダ３に送信する。コンテンツプロバイダ２はまた、取扱方針、および署名にコンテンツプロバイダ２の証明書を付して、EMDサービスセンタ１に送信する。

【００７６】

サービスプロバイダ３は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図１５を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ３の証明書（その詳細は図１６を参照して後述する）を付して、ユーザホームネットワーク５に送信する。サービスプロバイダ３はまた、価格情報、および署名にサービスプロバイダ３の証明書を付して、EMDサービスセンタ１に送信する。

【００７７】

ユーザホームネットワーク５は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク５において、コンテンツ鍵Ｋｃｏが復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ１に送信される。

【００７８】

EMDサービスセンタ１は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３それぞれの利益を算出する。EMDサービスセンタ１は、さらに、コンテンツプロバイダ２から受信した取扱方針、サービスプロバイダ３から受信した価格情報、並びにユーザホームネットワーク５から受信した課金情報および取扱方針を

比較し、サービスプロバイダ３またはユーザホームネットワーク５で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【００７９】

図１３は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００８０】

図１４は、コンテンツプロバイダ２の証明書を説明する図である。コンテンツプロバイダ２の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダの公開鍵Ｋｐｃｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、並びにコンテンツプロバイダの公開鍵Ｋｐｃｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００８１】

図１５は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００８２】

図１６は、サービスプロバイダ３の証明書を説明する図である。サービスプロバイダ３の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００８３】

図１７は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ２が有する取扱方針（図１７（Ａ））は、コンテンツ毎に用意され、ユーザホームネットワーク５が利用可能な利用内容を示す。例えば、図１７（Ａ）の取り扱い方針は、ユーザホームネットワーク５がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【００８４】

図１８は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図１８（Ａ）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ１つのコピーを作成することを言う。シングルコピーの場合も、図１８（Ｂ）に示すように、コピーを更にコピーすることはできない（許されない）。

【００８５】

サービスプロバイダ３は、図１７（Ｂ）に示すように、コンテンツプロバイダ２からの取扱方針（図１７（Ａ））に価格情報を加える。例えば、図１７（Ｂ）の価格情報は、そのコンテンツを再生して利用するときの料金が１５０円で、マルチコピーして利用するときの利用料金が８０円であることを示す。図１７には、例示しないが、シングルコピーの価格情報は、コピーの１回当たりの使用料金を表し、例えば、３回のコピーの利用では、シングルコピーの使用料金の３倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【００８６】

ユーザホームネットワーク５は、サービスプロバイダ３から供給される取扱方針が示すコンテンツの利用可能な利用内容（図１７（Ｂ））から、ユーザが選択した、利用内容を示す使用許諾条件情報（図１７（Ｃ））を記憶する。例えば、図１７（Ｃ）の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【００８７】

図１９は、図１７の例と比較してコンテンツプロバイダ２が取扱方針に利益分配の情報を加え、サービスプロバイダ３が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図１７に示す例に対して、図１９の例では、コンテンツプロバイダ２の利益が、コンテンツを再生して利用するとき７０円で、マルチコピーして利用するとき４０円であることを示す情報が、追加されている（図１９（Ａ））。更に、利益分配情報として、サービスプロバイダ３の利益が、コンテンツを再生して利用するとき６０円で、マルチコピーして利用するとき３０円であることが、追加されている（図１９（Ｂ））。価格は、図１７（Ａ）における場合と同様に、再生が１５０円、マルチコピーが４０円とされている。価格（例えば１５０円）からコンテンツプロバイダ２の利益（例えば７０円）およびサービスプロバイダ３の利益（例えば６０円）を差し引いた金額（例えば２０円）が、EMDサービスセンタ１の利益である。EMDサービス

センタ１は、ユーザホームネットワーク５のコンテンツの利用結果を示す課金情報（図１９（Ｃ））とともに、ユーザホームネットワーク５を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１のそれぞれの利益を算出できる。

【００８８】

図２０は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図２０（Ａ）の例では、サービスプロバイダ３において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、５回）のある再生、および期日制限（この例の場合、１９９８年１２月３１日まで）のある再生が設定されている。ユーザが、５回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ１度も再生していない状態では、図２０（Ｂ）に示すように、ユーザホームネットワーク５の使用許諾条件情報の回数制限に対応する値には、”５”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク５において、コンテンツが再生（利用）される度にデクリメントされ、例えば、３回再生された後、その値は、図２０（Ｃ）に示すように”２”とされる。回数制限に対応する値が、”０”となった場合、ユーザホームネットワーク５は、それ以上、そのコンテンツを再生して利用することができない。

【００８９】

図２１は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報の他の例を説明する図である。図１２に示した例に対して、図２１の例では、サービスプロバイダ３は、コンテンツプロバイダ２からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク５に送信され、EMDサービスセンタ１にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク５からEMDサービスセンタ１に送信される。

【００９０】

図２２は、図２１の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００９１】

図２３は、図２１の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図２３に示す例の場合、コンテンツプロバイダ２の取扱方針（図２３（Ａ））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ３は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク５に送信する（図２３（Ｂ））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図２３（Ｃ））を生成する。図２３のコンテンツプロバイダ２は、図１２の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【００９２】

図２４は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図２１に示した例に対して、図２４の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図２４のシステムは、図２１の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【００９３】

図２５は、図２４の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および配送用鍵Ｋｄで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００９４】

図２６は、図２４の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、配送用鍵Ｋｄで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、および配送用鍵Ｋｄで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００９５】

図２７は、EMDサービスセンタ１が、ユーザホームネットワーク５から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク５と相互認証した後、ユーザ管理部１８は、一時鍵Ｋｔｅｍｐを共有化し、鍵サーバ１４からの配送用鍵Ｋｄをこの鍵で暗号化しユーザホームネットワーク５に送信する。ユーザホームネットワーク５は、受信した配送用鍵Ｋｄを共有化した一時鍵Ｋｔｅｍｐで復号した後、配送用鍵Ｋｄを必要に応じて更新する。また、共有化した一時鍵Ｋｔｅｍｐを用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ１に送信する。ユーザ管理部１８はこれを受信する。ユーザ管理部

１８は、受信した課金情報、および取扱方針等を共有化した一時鍵Ｋｔｅｍｐで復号化した後、経歴データ管理部１５および課金請求部１９に送信する。経歴データ管理部１５は決済を実行すると判定した場合、受信した課金情報を利益分配部１６に送信し、さらに、受信した課金情報および取扱方針等を課金請求部１９に送信する。利益分配部１６は、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１自身に対する請求金額および支払金額を算出する。課金請求部１９は、ユーザの支払い金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部１９およびユーザ管理部１８に送信され、以後のユーザの登録処理時、または配送用鍵Ｋｄの送信処理時に参照される。

【００９６】

図２８は、EMDサービスセンタ１の利益分配処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部１６に送信する。利益分配部１６は、これらの情報を基に、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１それぞれの利益を算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部１１は、サービスプロバイダ３の利益の情報をサービスプロバイダ３に送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２の利益の情報をコンテンツプロバイダ２に送信する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【００９７】

図２９は、EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部１３および利益分配部１６に送信する。利益分配部１６は、JASRACに対する請求金額および支払金額を算出し

、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部１３は、ユーザのコンテンツの使用実績をJASRACに送信する。

【００９８】

次に、EMDシステムの処理について説明する。図３０は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップＳ１１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する。その処理の詳細は、図３２のフローチャートを参照して後述する。ステップＳ１２において、ユーザは、ユーザホームネットワーク５の機器（例えば、図１０のレシーバ５１）を操作し、ユーザホームネットワーク５の機器をEMDサービスセンタ１のユーザ管理部１８に登録する。この登録処理の詳細は、図３６のフローチャートを参照して後述する。ステップＳ１３において、EMDサービスセンタ１のユーザ管理部１８は、ユーザホームネットワーク５と、図３３乃至図３５に示したように相互認証した後、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを送信する。ユーザホームネットワーク５はこの鍵を受信する。この処理の詳細は、図４５のフローチャートを参照して説明する。

【００９９】

ステップＳ１４において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図４７のフローチャートを参照して後述する。ステップＳ１５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、ユーザホームネットワーク５からの要求に応じて、ネットワーク４を介して、ユーザホームネットワーク５にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図４９のフローチャートを参照して後述する。ステップＳ１６において、ユーザホームネットワーク５の課金モジュール７２は、課金処理を実行する。課金処理の詳細は、図５１のフローチャートを参照して後述する。ステップＳ１７において、ユーザは、ユーザホームネットワーク５の機器でコンテンツを再生する。再生処理の詳細は、図５２のフローチャートを参照して

後述する。

【０１００】

一方、コンテンツプロバイダ２が、取扱方針を暗号化して送信する場合の処理は、図３１のフローチャートで示すようになる。ステップＳ２１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信する。ステップＳ２２において、EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ３に配送用鍵Ｋｄを送信する。それ以降のステップＳ２３乃至ステップＳ２８の処理は、図３０のステップＳ１２乃至ステップＳ１７の処理と同様の処理であり、その説明は省略する。

【０１０１】

図３２は、図３０のステップＳ１１および図３１のステップＳ２１に対応する、EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する処理の詳細を説明するフローチャートである。ステップＳ３１において、EMDサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２の相互認証部３９と相互認証する。この相互認証処理の詳細は、図３３を参照して後述する。相互認証処理により、コンテンツプロバイダ２が、正当なプロバイダであることが確認されたとき、ステップＳ３２において、コンテンツプロバイダ２の暗号化部３４および暗号化部３６は、EMDサービスセンタ１のコンテンツプロバイダ管理部１２から送信された配送用鍵Ｋｄを受信する。ステップＳ３３において、コンテンツプロバイダ２の暗号化部３４は、受信した配送用鍵Ｋｄを記憶する。

【０１０２】

このように、コンテンツプロバイダ２は、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。同様に、図３１に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ２以外に、サービスプロバイダ３も、図３２と同様の処理で、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。

【０１０３】

次に、図３２のステップＳ３１における、いわゆるなりすましがないことを確

認する相互認証の処理について、１つの共通鍵を用いる（図３３）、２つの共通鍵を用いる（図３４）、および公開鍵暗号を用いる（図３５）を例として説明する。

【０１０４】

図３３は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋcで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１０５】

ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋcで復号する。ステップＳ４５において、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いて$R1_H \| R2$を共通鍵Ｋcで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化した$R1_H \| R2$をコンテンツプロバイダ２に送信する。

【０１０６】

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$R1_H \| R2$を共通鍵Ｋcで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$R1_H \| R2$の上位３２ビット$R1_H$

を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$R1_H$と一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数$R1_H$と、受信した$R1_H$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋcで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１０７】

ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Ｋcで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１０８】

図３４は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１０９】

ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５におい

て、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１１０】

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１１１】

ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１１２】

図３５は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成す

る。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１３】

ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１１４】

適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（

認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１１５】

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１１６】

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１７】

ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、

ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなけば、不適正なプロバイダとして、処理を終了する。

【０１１８】

以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１１９】

図３６は、図３０のステップＳ１２および図３１のステップＳ２３に対応する、レシーバ５１がEMDサービスセンタ１のユーザ管理部１８に登録する処理を説明するフローチャートである。ステップＳ１０１において、レシーバ５１のSAM６２は、ICカードインターフェース６４の出力から、レシーバ５１にバックアップ用のICカード５５が装着されているか否かを判定し、バックアップ用のICカード５５が装着されていると判定された場合（例えば、レシーバ５１が新たなレシーバ５１に変更され、元のレシーバ５１のデータを、新たなレシーバ５１に引き継ぐために、元のレシーバ５１のデータをバックアップ用のICカード５５にバックアップさせている場合）、ステップＳ１０２に進み、ICカード５５に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図４１のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード５５に、バックアップデータを記憶させる必要があるが、その処理は、図３９を参照して後述する。

【０１２０】

ステップＳ１０１において、バックアップ用のICカード５５が装着されていないと判定された場合、手続は、ステップＳ１０２をスキップし、ステップＳ１０３に進む。ステップＳ１０３において、SAM６２の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証し、SAM６２は、証明書をEMDサービスセンタ１のユーザ管理部１８に送信する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１０３で、SAM６２がEMDサービスセンタ１のユーザ管理部１８に送信する

証明書は、図３７に示すデータを含む。SAM６２が送信する証明書は、図１４に示すコンテンツプロバイダ２の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップＳ１０４において、SAM６２は、通信部６１を介して、一時鍵Ｋｔｅｍｐで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１２１】

ステップＳ１０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したSAM６２のIDを基に、図７に示したユーザ登録データベースを検索する。ステップＳ１０６において、EMDサービスセンタ１のユーザ管理部１８は、受信したIDを有するSAM６２の登録が可能であるか否かを判定し、受信したIDを有するSAM６２の登録が可能であると判定された場合、ステップＳ１０７に進み、受信したIDを有するSAM６２が、新規登録であるか否かを判定する。ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録ではないと判定された場合、手続は、ステップＳ１０８に進む。

【０１２２】

ステップＳ１０８において、EMDサービスセンタ１のユーザ管理部１８は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図３８に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ１のユーザ管理部１８が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵Ｋｃｏの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化した署名から構成される。

【０１２３】

機器のSAMのIDは、機器の固有の６４ビットからなるIDを示す（図３８では、１６進数で示す）。登録拒絶フラグの”１”は、EMDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”０”は、MDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器の

登録を拒絶したことを示す。

【０１２４】

ステータスフラグのMSB(Most Significant Bit)の”１”は、対応するIDを有する子の機器（例えばレコーダ５３）が従属した親の機器（例えばレシーバ５１）からコンテンツ鍵Ｋｃｏをもらえることを示し、ステータスフラグのMSBの”０”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵Ｋｃｏをもらえないことを示している。ステータスフラグの上位から２ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグの上位から３ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”１”は、従属した親の機器が配送用鍵Ｋｄで暗号化したコンテンツ鍵Ｋｃｏを購入し、対応するIDを有する子の機器に、一時鍵Ｋｔｅｍｐで暗号化してコンテンツ鍵Ｋｃｏを渡すことを示す。

【０１２５】

コンディションフラグの”０”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来る（すなわち、例えばレシーバ５１のような親の機器である）ことを示し、コンディションフラグの”１”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来ない（すなわち、例えばレコーダ５３のような子の機器である）ことを示す。コンディションフラグが”０”のとき、ステータスフラグは常に”００００”に設定される。

【０１２６】

ステップＳ１０９において、EMDサービスセンタ１のユーザ管理部１８は、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで暗号化した、鍵サーバ１４から供給された配送用鍵Ｋｄをレシーバ５１のSAM６２に送信する。ステップＳ１１０において、レシーバ５１のSAM６２は、受信した配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させる。

【０１２７】

ステップＳ１１１において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化した登録リストをレシーバ５１のSAM６２に送信する。ステップＳ１１２において、レシーバ５１のSAM６２は、受信した登録リストを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させ、処理は終了する。

【０１２８】

ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録であると判定された場合、手続は、ステップＳ１１４に進み、EMDサービスセンタ１のユーザ管理部１８は、新規登録を実行し、登録リストを作成し、ステップＳ１０９に進む。

【０１２９】

ステップＳ１０６において、受信したIDを有するSAM６２の登録が不可であると判定された場合、ステップＳ１１３に進み、EMDサービスセンタ１のユーザ管理部１８は、登録拒絶の登録リストを作成し、ステップＳ１１１に進む。

【０１３０】

このように、レシーバ５１は、EMDサービスセンタ１に登録される。

【０１３１】

次に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる処理の詳細を、図３９のフローチャートを参照して説明する。ステップＳ１２１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１２２において、SAM６２の乱数発生ユニット９２は、バックアップ鍵Ｋｉｃとして用いられる乱数を生成する。ステップＳ１２３において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、バックアップ鍵Ｋｉｃを用いて暗号化する。ステップＳ１２４において、SAM６２の暗号化ユニット９３は、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃでバックアップ鍵Ｋｉｃを暗号化する（SAM６２は、EMDサービスセンタ１との間の認証

処理（図３５のステップＳ８９）において、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを取得している）。ステップＳ１２５において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のID並びに暗号化されたバックアップ鍵ＫｉｃをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３２】

以上のように、SAM６２の記憶モジュール７３に記憶されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、バックアップ鍵Ｋｉｃを用いて暗号化され、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたバックアップ鍵Ｋｉｃと共に、ICカード５５の記憶モジュール８１に記憶される。

【０１３３】

今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる他の処理の例の詳細を、図４０のフローチャートを参照して説明する。ステップＳ１３１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。ステップＳ１３２において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化する。ステップＳ１３３において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３４】

図４０に示す処理により、図３９に示した場合より簡単な処理で、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、ICカード５５の記憶モジュール８１に記憶される。

【０１３５】

このように、ICカード５５にバックアップされたデータは、図３６のステップＳ１０２の処理で、新しいレシーバ５１に読み込まれる。図４１は、図３９に示

す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップＳ１４１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１３６】

ステップＳ１４２において、SAM６２は、ICカードインタフェース６４を介して、記憶モジュール８１に記憶された、バックアップ鍵Ｋｉｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを読み出す。ステップＳ１４３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１４４において、SAM６２は、通信部６１を介して、バックアップ鍵Ｋｉｃで暗号化されている記憶モジュール７３のデータ、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１３７】

ステップＳ１４５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１４６において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップデータを、バックアップ鍵Ｋｉｃで復号する。ステップＳ１４７において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１４８において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１３８】

ステップＳ１４９において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１５０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１３９】

このように、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１４０】

また、図３６のステップＳ１０２は、図４２に示すフローチャートで説明される処理でもよい。ステップＳ１６１乃至ステップＳ１６３は、図４１のステップＳ１４１乃至ステップＳ１４３とそれぞれ同様であるので、その説明は省略する。ステップＳ１６４において、SAM６２は、通信部６１を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４１】

ステップＳ１６５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１６６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップ鍵Ｋｉｃを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１６７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップ鍵Ｋｉｃを、レシーバ５１の通信部６１に送信し、バックアップ鍵Ｋｉｃの復号のサービスに対するユーザへの課金の処理をする。

【０１４２】

ステップＳ１６８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信した一時鍵Ｋｔｅｍｐで暗号化されたバックア

ップ鍵Ｋｉｃを、SAM６２に送信し、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップ鍵Ｋｉｃを復号する。ステップＳ１６９において、SAM６２は、復号されたバックアップ鍵Ｋｉｃで、ステップＳ１６２においてICカード５５から読み出された古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を復号し、記憶モジュール７３に記憶させる。ステップＳ１７０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１４３】

図４２に示した読み込みの処理は、図４１に示した処理に比較し、レシーバ５１とEMDサービスセンタ１の送受信されるデータの量が少なくでき、従って、通信時間を短くできる。図４１のステップＳ１４８において、図４２のステップＳ１６７と同様に、EMDサービスセンタ１は、課金の処理を行ってもよい。

【０１４４】

図４０に示す処理でバックアップされたデータ読み出す場合の処理を、図４３に示すフローチャートを用いて説明する。ステップＳ１８１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１８２において、SAM６２は、ICカードインタフェース６４を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を読み出す。

【０１４５】

ステップＳ１８３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１８４において、SAM６２は、通信部６１を介して

、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている記憶モジュール７３のデータを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４６】

ステップＳ１８５において、EMDサービスセンタ１のユーザ管理部１８は、受信した記憶モジュール７３のデータを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１８６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１８７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１４７】

ステップＳ１８８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そにのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１８９において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定する。

【０１４８】

このように、図４０に示す処理を用いたバックアップの場合、図４３に示す処理により、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１４９】

レシーバ５１は、自分自身を登録する場合（図３０のステップＳ１２に対応する処理を実行する場合）、図３６のフローチャートに示す処理を実行するが、レシーバ５１に従属するレコーダ５３をEMDサービスセンタ１に登録する場合、図４４のフローチャートに示す処理を実行する。ステップＳ２０１において、レシーバ５１のSAM６２は、記憶モジュール７３に記憶された登録リストに、レコーダ５３のIDを書き込む。ステップＳ２０２において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この

認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１５０】

ステップＳ２０３において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のID（図３７に示すSAM６２の証明書に含まれるSAM６２のID）を基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ２０４に進み、レシーバ５１のSAM62は、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報（後述の図５１に示すフローチャートのステップＳ３５７の処理で記憶される）、および登録リスト、並びにHDD５２に記録された取扱方針を一時鍵Ｋｄで暗号化し、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、並びにHDD５２に記録された取扱方針を送信する。ステップＳ２０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図３８を参照して説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１５１】

ステップＳ２０６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新か否かを判定し、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新であると判定された場合、ステップＳ２０７に進み、一時鍵Ｋｄで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ２０８において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ２０７において受信したものに更新し、ステップＳ２１１に進む。

【０１５２】

ステップＳ２０６において、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新のものではないと判定された場合、ステップＳ２０９に進み、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｄで暗号化した、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ２１０において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ２０９において受信したものに更新し、配送用鍵Ｋｄを最新バージョンのものに更新し、ステップＳ２１１に進む。

【０１５３】

ステップＳ２１１において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２１２に進み、レシーバ５１とレコーダ５３は相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２１３において、レコーダ５３に、一時鍵Ｋｄで暗号化した、登録完了メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、登録完了メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２１４において、レコーダ５３は、配送用鍵Ｋｄを更新し、処理は終了する。

【０１５４】

ステップＳ２０３において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ２１１において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１５５】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、EMDサービスセンタ１に登録される。

【０１５６】

図４５は、図３０のステップＳ１３において、EMDサービスセンタ１がレシーバ５１に送信した配送用鍵Ｋｄを、レシーバ５１が受け取る処理の詳細を説明するフローチャートである。ステップＳ２２１において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２２２において、レシーバ５１のSAM６２は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に証明書を送信し、EMDサービスセンタ１のユーザ管理部１８は、証明書を受信する。ステップＳ２２３乃至ステップＳ２３０は、図４４のステップＳ２０３乃至ステップＳ２１０と同様の処理であるのでその説明は省略する。

【０１５７】

このように、レシーバ５１は、EMDサービスセンタ１のユーザ管理部１８から配送用鍵Ｋｄを受け取り、レシーバ５１の課金情報をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１５８】

次に、レシーバ５１に従属するレコーダ５３の配送用鍵Ｋｄの受け取り処理（図３８に示すステータスフラグが、レコーダ５３の配送用鍵Ｋｄの受け取りを許可する値を有する場合）を、図４６に示すフローチャートを用いて説明する。ステップＳ２４１において、レシーバ５１の相互認証モジュール７１およびレコーダ５３の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１５９】

ステップＳ２４２において、レシーバ５１は、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っているか否かを判定し、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていると判定された場合、ステップＳ２４３に進み、レシーバ５１の記憶モジュール７３に記憶する登録リストを基に、レコーダ５３が登録不可であ

るか否かを判定する。ステップＳ２４３において、レコーダ５３が登録不可ではないと判定された場合、ステップＳ２４４に進み、レコーダ５３のSAM６６は、レシーバ５１のSAM６２に、内蔵する記憶モジュールに記憶している配送用鍵Ｋｄ（後述する図４６のステップＳ２５５でレシーバ５１から受け取っている）のバージョンおよび課金情報（後述する図５１に対応する処理のステップＳ３５７に相当する処理で記憶している）を一時鍵Ｋｔｅｍｐで暗号化して、送信し、レシーバ５１のSAM６２は、配送用鍵Ｋｄのバージョンおよび課金情報を受信し、復号する。

【０１６０】

ステップＳ２４５において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と、相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２４６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のIDを基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ２４７に進み、レシーバ５１のSAM62は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、一時鍵Ｋｄで暗号化した、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、HDD５２に記録している取扱方針、並びにレコーダ５３の課金情報を送信する。ステップＳ２４８において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図３８で説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１６１】

ステップＳ２４９乃至ステップＳ２５４の処理は、図４４に示すステップＳ２０６乃至ステップＳ２１１とそれぞれ同様であるので、その説明は省略する。

【０１６２】

ステップＳ２５４において、レシーバ５１のSAM６２は、更新した登録リスト

を参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２５５に進み、レコーダ５３に、一時鍵Ｋｄで暗号化した、課金情報受信メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、課金情報受信メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２５６において、レコーダ５３のSAM６６は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Ｋｄを最新のバージョンに更新する。

【０１６３】

ステップＳ２４２において、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていないと判定された場合、ステップＳ２５７に進み、図４４に示したレコーダ５３の登録処理を実行し、ステップＳ２４４に進む。

【０１６４】

ステップＳ２４３において、レコーダ５３が登録不可であると判定された場合、ステップＳ２４６において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ２５４において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１６５】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、配送用鍵Ｋｄを受け取る。

【０１６６】

次に、図３０のステップＳ１４に対応する、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を、図４７のフローチャートを用いて説明する。ステップＳ２７１において、コンテンツプロバイダ２のウォータマーク付加部３２は、コンテンツサーバ３１から読み出したコンテンツに、コンテンツプロバイダ２を示す所定のウォータマークを挿入し、圧縮部３３に供給する。ステップＳ２７２において、コンテンツプロバイダ２の圧縮部３３は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップS-2７３において、乱数発

生部３５は、コンテンツ鍵Ｋｃｏとして用いる乱数を発生させ、暗号化部３４に供給する。ステップＳ２７４において、コンテンツプロバイダ２の暗号化部３４は、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏを使用して、ウォータマークが挿入され、圧縮されたコンテンツを暗号化する。

【０１６７】

ステップＳ２７５において、暗号化部３６は、DESなどの所定の方式で、図３０のステップＳ１１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを暗号化する。ステップＳ２７６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、およびポリシー記憶部３７から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図１３に示すような署名を作成する。ステップＳ２７７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、ポリシー記憶部３７から供給される取扱方針、およびステップＳ２７６で生成した署名を含んだ、図１３に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【０１６８】

ステップＳ２７８において、コンテンツプロバイダ２の相互認証部３９は、サービスプロバイダ３の相互認証部４５と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２７９において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【０１６９】

以上のように、コンテンツプロバイダ２は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナを送信する。

【０１７０】

コンテンツ鍵Ｋｃｏと共に取扱方針を配送用鍵Ｋｄで暗号化する例の場合の、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュ

アコンテナを送信する他の処理の詳細を、図４８のフローチャートを用いて説明する。ステップＳ２９１乃至ステップＳ２９４の処理は、図４７のステップＳ２７１乃至ステップＳ２７４の処理とそれぞれ同様であり、その説明は省略する。ステップＳ２９５において、コンテンツプロバイダ２の暗号化部３６は、図３１のステップＳ２１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄを用いて、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏおよびポリシー記憶部３７から供給される取扱方針を暗号化する。

【０１７１】

ステップＳ２９６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図２５に示すような署名を作成する。ステップＳ２９７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、暗号化された取扱方針、および署名を含んだ、図２５に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップＳ２９８およびステップＳ２９９の処理は、図４７のステップＳ２７８およびステップＳ２７９の処理とそれぞれ同様であり、その説明は省略する。

【０１７２】

このように、コンテンツプロバイダ２は、サービスプロバイダ３に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【０１７３】

次に、図３０のステップＳ１５に対応する、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を図４９のフローチャートを用いて説明する。ステップＳ３１１において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ２の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図３５のステップＳ８３における

処理と同様であるので、その説明は省略する。

【０１７４】

ステップＳ３１２において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【０１７５】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップＳ３１３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップＳ３１４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図１７で説明した価格情報を作成する。ステップＳ３１５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵Ｋｓｓｐで暗号化し、得られた値を署名として図１５に示すようなサービスプロバイダセキュアコンテナを作成する。

【０１７６】

ステップＳ３１６において、サービスプロバイダ３の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ３１７において、サービスプロバイダ３のセキュアコンテナ作成部４４は、レシーバ５１の通信部６１に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【０１７７】

このように、サービスプロバイダ３は、レシーバ５１にサービスプロバイダセ

キュアコンテナを送信する。

【０１７８】

コンテンツプロバイダ２において、取扱方針が配送用鍵Ｋｄで暗号化され、かつ、サービスプロバイダ３が取扱制御情報を作成する例の場合の、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図５０のフローチャートを用いて説明する。ステップＳ３３１およびステップＳ３３２の処理は、図４９のステップＳ３１１およびステップＳ３１２の処理とそれぞれ同様であるので、その説明は省略する。ステップＳ３３３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップＳ３３４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図２３で説明した取扱制御情報を作成する。ステップＳ３３５乃至ステップＳ３３８の処理は、図４９のステップＳ３１４およびステップＳ３１７の処理とそれぞれ同様であるので、その説明は省略する。

【０１７９】

このように、サービスプロバイダ３は、レシーバ５１に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【０１８０】

図３０のステップＳ１６に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ５１の課金処理の詳細を、図５１のフローチャートを用いて説明する。ステップＳ３５１において、レシーバ５１の復号／暗号化モジュール７４は、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できるか否かを判定し、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できないと判定された場合、ステップＳ３５２で、レシーバ５１は、図４５で説明した配送用鍵Ｋｄの受け取り処理を実行し、ステップＳ３５３に進む。ステップＳ３５１において、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できると判定された場合、手続は、ステップＳ３５２をスキップし、ステップＳ３５３に進む。ステップＳ３５３において、レシーバ５１の復号ユニット９１は、図３０のステップＳ１３の処理により、記憶モジュール７３に記憶されている配送用鍵Ｋｄで、コンテンツ鍵Ｋｃｏを復号す

る。

【０１８１】

ステップＳ３５４において、レシーバ５１の課金処理モジュール７２は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図１９および図２０で説明した課金情報および使用許諾条件情報を生成する。ステップＳ３５５において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に記憶している課金情報およびステップＳ３５４で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップＳ３５６に進み、レシーバ５１は図４５で説明した配送用鍵Ｋｄの受け取り処理を実行し、新たな配送用鍵Ｋｄを受け取り、ステップＳ３５７に進む。ステップＳ３５５において、現在の課金が課金の上限未満であると判定された場合、ステップＳ３５６はスキップされ、ステップＳ３５７に進む。

【０１８２】

ステップＳ３５７において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に課金情報を記憶させる。ステップＳ３５８において、レシーバ５１の課金処理モジュール７２は、ステップＳ３５４にて生成した使用許諾条件情報をHDD５２に記録する。ステップＳ３５９において、レシーバ５１のSAM６２は、HDD５２にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【０１８３】

ステップＳ３６０において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３６１において、レシーバ５１の記憶モジュール７３は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３６２において、レシーバ５１の乱数発生ユニット９２は、保存用鍵Ｋｓａｖｅである乱数を発生し、ステップＳ３６３に進む。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３６２はスキップされ、ステップＳ３６３に進む。

【０１８４】

ステップＳ３６３において、レシーバ５１の暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化する。ステップＳ３６４において、レシーバ５１のSAM６２は、暗号化されたコンテンツ鍵Ｋｃｏを HDD５２に記憶させる。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３６５において、レシーバ５１の復号／暗号化モジュール７４は、保存用鍵Ｋｓａｖｅを記憶モジュール７３に記憶させ、処理は終了する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３６５はスキップされ、処理は終了する。

【０１８５】

以上のように、レシーバ５１は、課金情報を記憶モジュール７３に記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、記憶モジュール７３に記憶されている。

【０１８６】

レコーダ５３も、同様の処理で、課金情報をSAM６６内の記憶モジュールに記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、SAM６６内の記憶モジュールに記憶されている。

【０１８７】

図３０のステップＳ１７に対応するレシーバ５１がコンテンツを再生する処理の詳細を、図５２のフローチャートを用いて説明する。ステップＳ３８１において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２から、図５１のステップＳ３５８で記憶した使用許諾条件情報およびステップＳ３６４で記憶した暗号化されたコンテンツ鍵Ｋｃｏを読み出す。ステップＳ３８２において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【０１８８】

ステップＳ３８３において、レシーバ５１の復号／暗号化モジュール７４は、

ステップＳ３８２において算出されたハッシュ値が、図５１のステップＳ３６０で記憶モジュール７３に記憶されたハッシュ値と一致するか否かを判定し、ステップＳ３８２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致すると判定された場合、ステップＳ３８４に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップＳ３８５において、レシーバ５１の復号／暗号化モジュール７４は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３８６において、レシーバ５１の記憶モジュール７３は、ステップＳ３８５で算出した使用許諾条件情報のハッシュ値を記憶する。ステップＳ３８７において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２に更新した使用許諾条件情報を記録させる。

【０１８９】

ステップＳ３８８において、SAM６２の相互認証モジュール７１と伸張部６３の相互認証モジュール７５は、相互認証し、SAM６２および伸張部６３は、一時鍵Ｋｔｅｍｐを記憶する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ３８９において、復号／暗号化モジュール７４の復号ユニット９１は、図５１のステップＳ３６４にてHDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ３９０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ３９１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを伸張部６３に送信する。

【０１９０】

ステップＳ３９２において、伸張部６３の復号モジュール７６は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ３９３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、伸張部６３に送信する。ステップＳ３９４において、伸張部６３の復号モジュール７７は、コンテンツをコン

テンツ鍵Ｋｃｏで復号する。ステップＳ３９５において、伸張部６３の伸張モジュール７８は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ３９６において、伸張部６３のウォータマーク付加モジュール７９は、伸張されたコンテンツにレシーバ５１を特定する所定のウォータマークを挿入する。ステップＳ３９７において、レシーバ５１は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０１９１】

ステップＳ３８３において、ステップＳ３８２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、ステップＳ３９８において、SAM６２は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０１９２】

このように、レシーバ５１は、コンテンツを再生する。

【０１９３】

図５３は、図１１の構成を有するユーザホームネットワーク５において、レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。ステップＳ４１１乃至ステップＳ４１７の処理は、図５２のステップＳ３８１乃至ステップＳ３８７の処理とそれぞれ同様であるので、その説明は省略する。

【０１９４】

ステップＳ４１８において、SAM６２の相互認証モジュール７１とデコーダ５６の相互認証モジュール１０１は、相互認証し、一時鍵Ｋｔｅｍｐが共有される。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ４１９において、復号／暗号化モジュール７４の復号ユニット９１は、HDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ４２０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ

４２１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏをデコーダ５６に送信する。

【０１９５】

ステップＳ４２２において、デコーダ５６の復号モジュール１０２は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ４２３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、デコーダ５６に送信する。ステップＳ４２４において、デコーダ５６の復号モジュール１０３は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ４２５において、デコーダ５６の伸張モジュール１０４は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ４２６において、デコーダ５６のウォータマーク付加モジュール１０５は、伸張されたコンテンツにデコーダ５６を特定する所定のウォータマークを挿入する。ステップＳ４２７において、デコーダ５６は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０１９６】

ステップＳ４２８の処理は、図５２のステップＳ３９８の処理と同様であるので、その説明は省略する。

【０１９７】

以上のように、ユーザホームネットワークが図１１に示す構成を有する場合、レシーバ５１が受信したコンテンツは、デコーダ５６で再生される。

【０１９８】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【０１９９】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【０２００】

さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【０２０１】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０２０２】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０２０３】

【発明の効果】

請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体によれば、装着された外部記憶媒体と相互認証し、所定の鍵で所定の情報を暗号化するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【０２０４】

請求項５に記載の管理装置、請求項６に記載の管理方法、および請求項７に記載の提供媒体によれば、情報処理装置に装着された外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【０２０５】

請求項８に記載の情報利用システムによれば、情報処理装置が、装着された外部記憶媒体と相互認証し、管理装置の公開鍵で所定の情報を暗号化し、管理装置が、外部記憶媒体に記憶されたデータを復号するようにしたので、不正に対する安全性を保持したまま、必要な情報を外部に記憶できる。

【０２０６】

請求項９に記載の外部記憶媒体によれば、情報処理装置と相互認証するようにしたので、不正な読み取りを防止できる。

【図面の簡単な説明】

【図１】

EMDのシステムを説明する図である。

【図２】

EMDサービスセンタ１の機能の構成を示すブロック図である。

【図３】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図４】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図６】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図７】

ユーザ登録データベースを説明する図である。

【図８】

コンテンツプロバイダ２の機能の構成を示すブロック図である。

【図９】

サービスプロバイダ３の機能の構成を示すブロック図である。

【図１０】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１１】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１２】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図１３】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図１４】

コンテンツプロバイダ２の証明書を説明する図である。

【図１５】

サービスプロバイダセキュアコンテナを説明する図である。

【図１６】

サービスプロバイダ３の証明書を説明する図である。

【図１７】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図１８】

シングルコピーおよびマルチコピーを説明する図である。

【図１９】

取扱方針および価格情報を説明する図である。

【図２０】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図２１】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２２】

サービスプロバイダセキュアコンテナを説明する図である。

【図２３】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図２４】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２５】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図２６】

サービスプロバイダセキュアコンテナを説明する図である。

【図２７】

EMDサービスセンタ１の、ユーザホームネットワーク５からの課金情報の受信のときの動作を説明する図である。

【図２８】

EMDサービスセンタ１の利益分配処理の動作を説明する図である。

【図２９】

EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

【図３０】

コンテンツの配布の処理を説明するフローチャートである。

【図３１】

コンテンツの配布の処理を説明するフローチャートである。

【図３２】

EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

【図３３】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３４】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３５】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３６】

レシーバ５１のEMDサービスセンタ１への登録の処理を説明するフローチャートである。

【図３７】

SAMの証明書を説明する図である。

【図３８】

登録リストを説明する図である。

【図３９】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４０】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４１】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４２】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４３】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４４】

レシーバ５１が、従属関係のあるレコーダ５３をEMDサービスセンタ１に登録する処理を説明するフローチャートである。

【図４５】

レシーバ５１がEMDサービスセンタ１から配送用鍵Ｋｄを受け取る処理を説明するフローチャートである。

【図４６】

レコーダの配送用鍵Ｋｄの受け取り処理を説明するフローチャートである。

【図４７】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図４８】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図４９】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５０】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５１】

レシーバ５１の課金処理を説明するフローチャートである。

【図５２】

レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図５３】

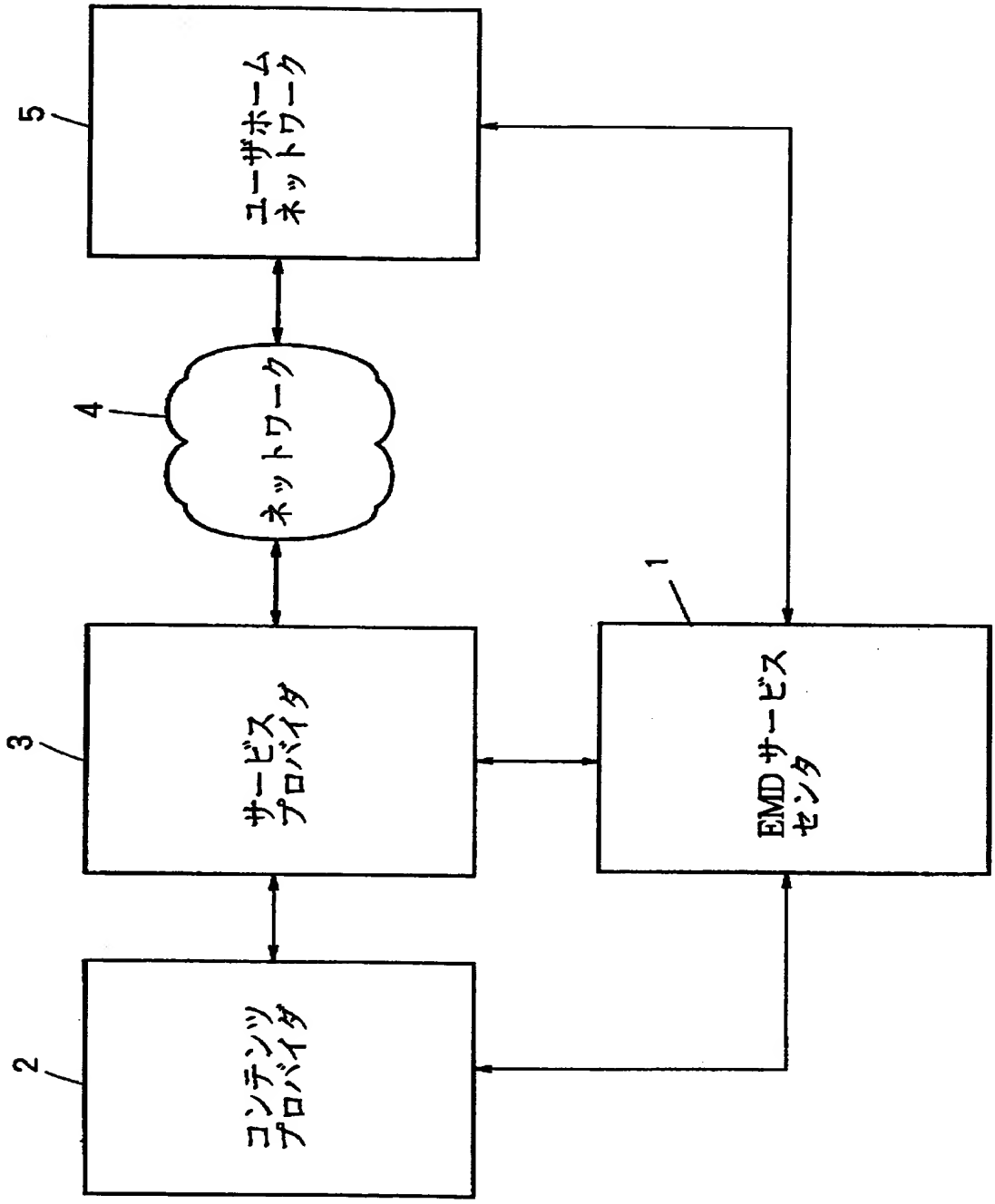
レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。

【符号の説明】

１　EMDサービスセンタ，　２　コンテンツプロバイダ、　３　サービスプロバイダ，５　ユーザホームネットワーク，　１６　利益分配部，　１８　ユーザ管理部，　４２　値付け部，　５１　レシーバ，　５６　デコーダ，　６１　通信部，　６２　SAM，　６３　伸張部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　相互認証モジュール，　７６　復号モジュール，　７７　復号モジュール，　８１　相互認証モジュール，　９１　復号ユニット，　９２　暗号化ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール

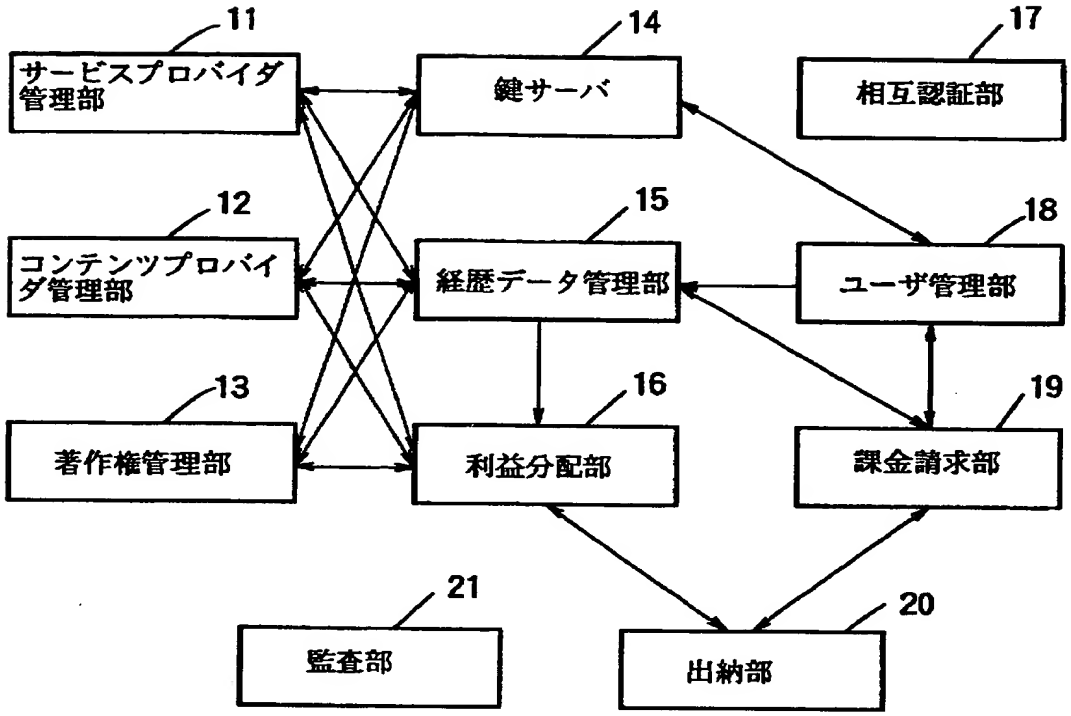
【書類名】　図面

【図１】



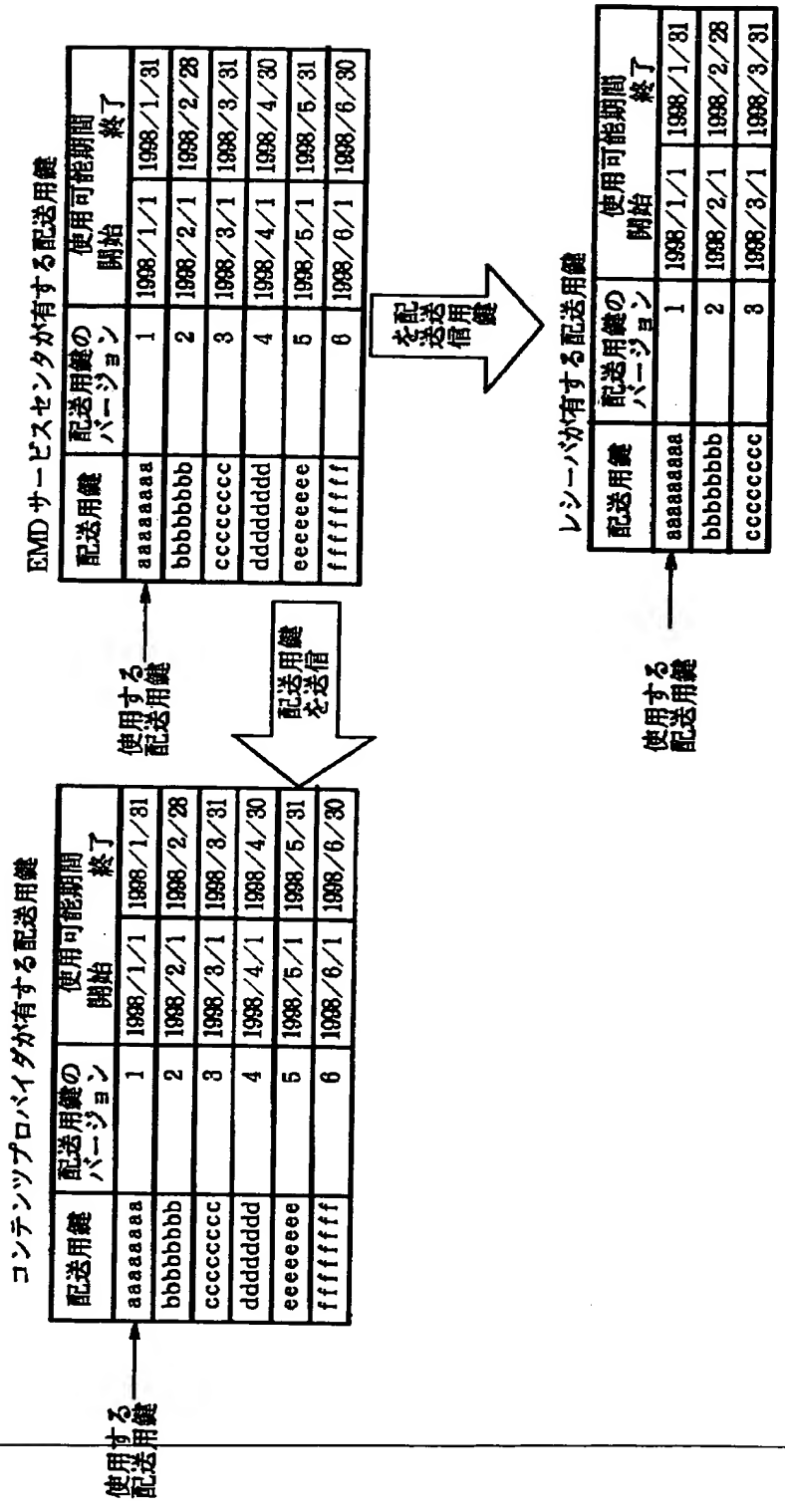
出証特平１１－３０５９１４４

【図２】

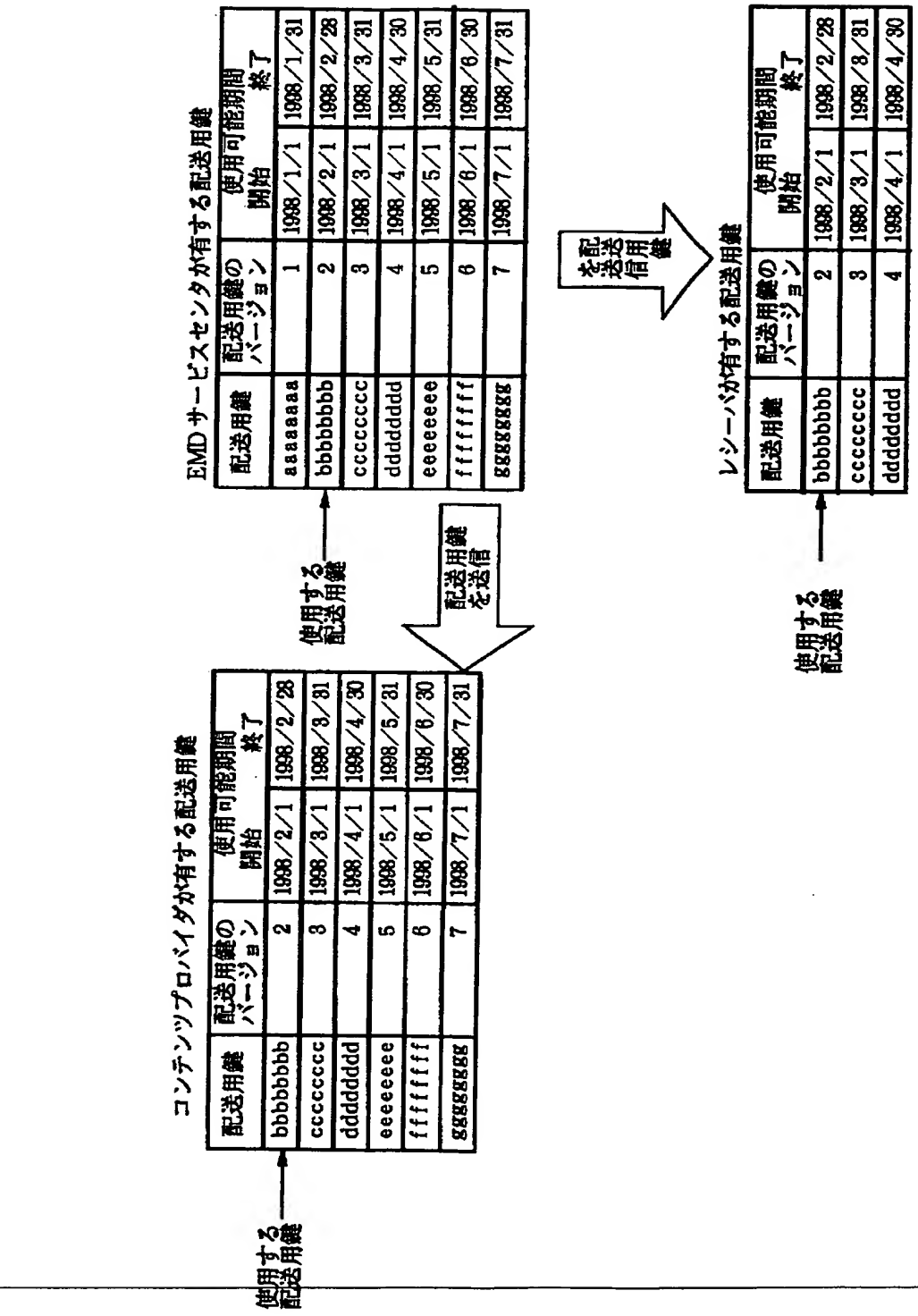


EMD サービスセンタ 1

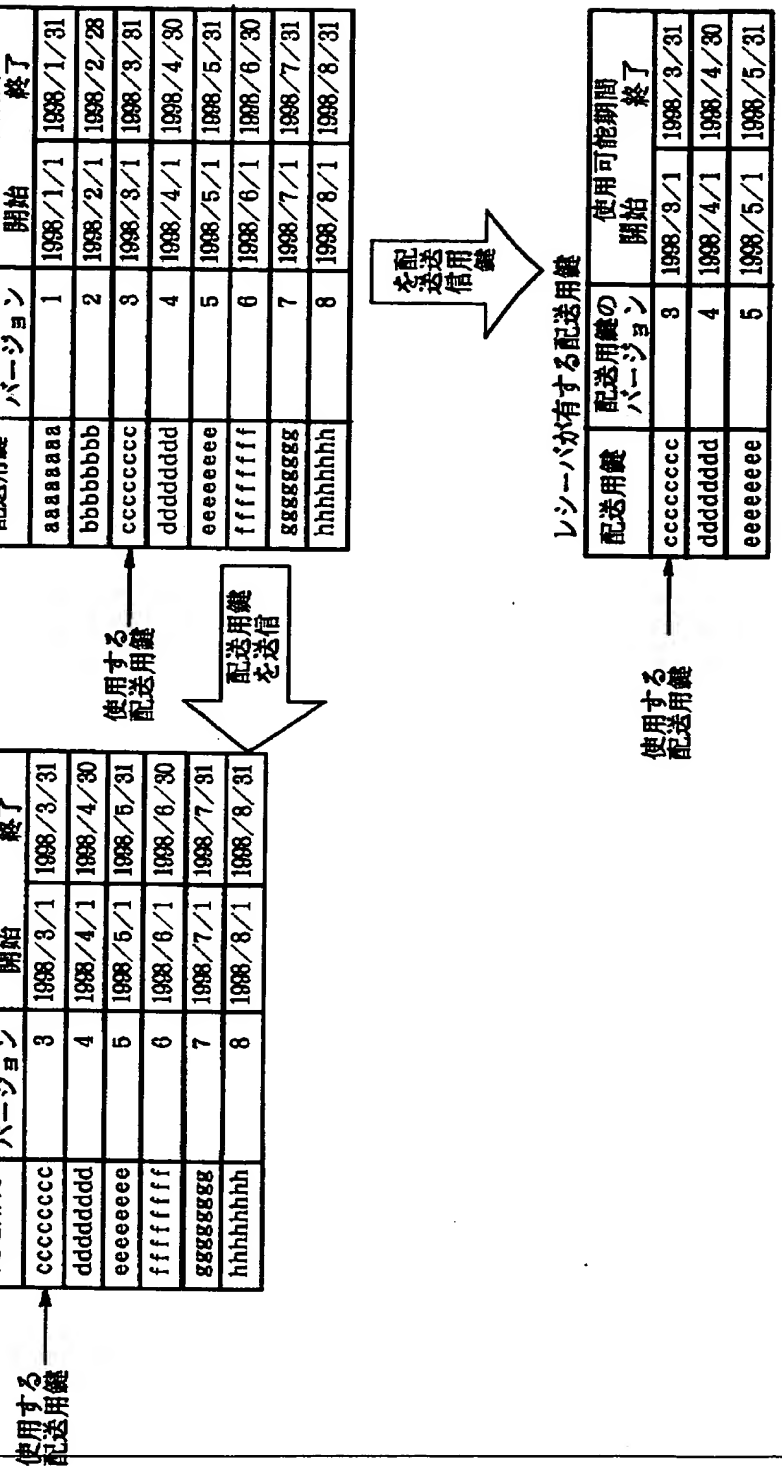
【図３】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

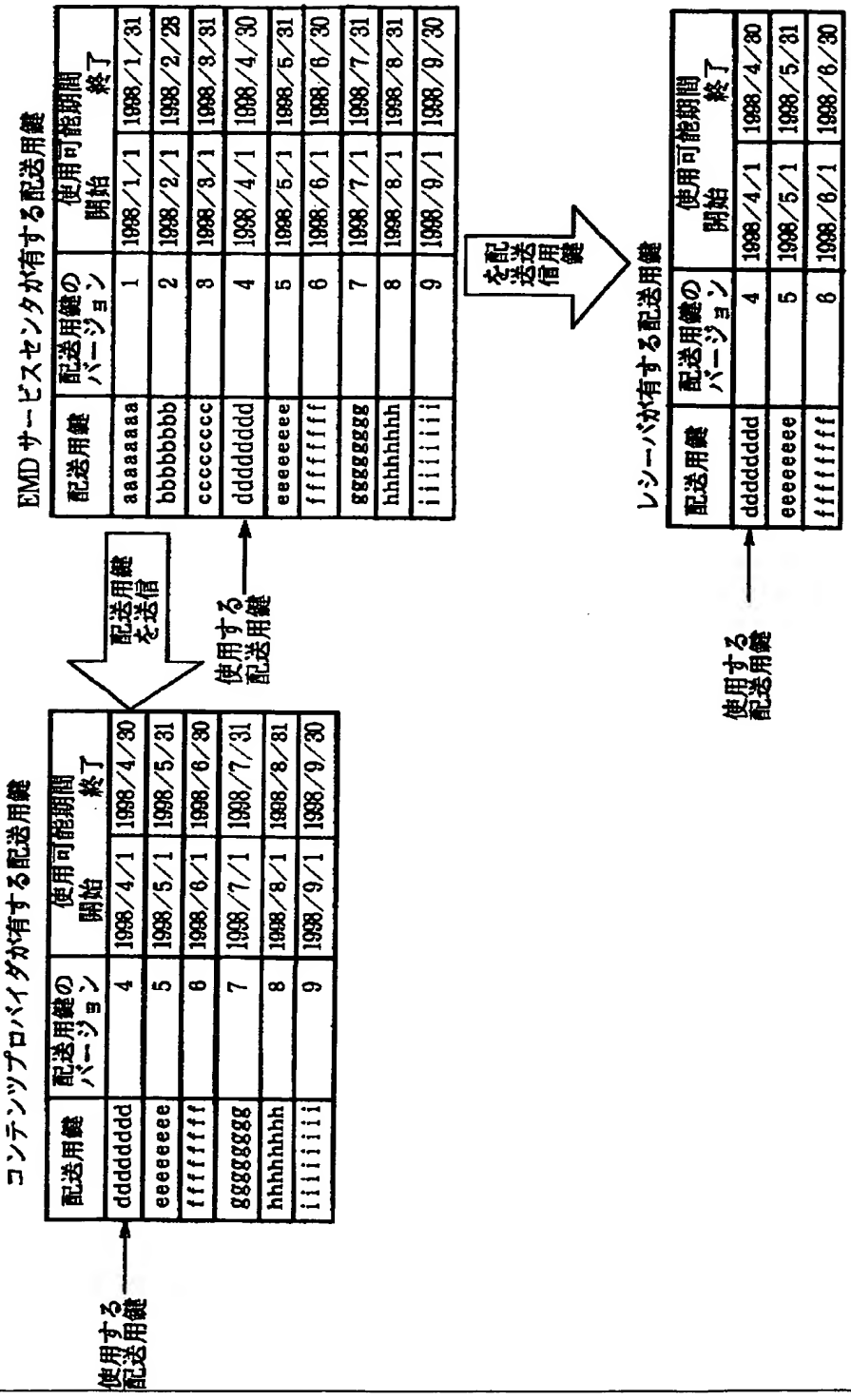
【図４】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵

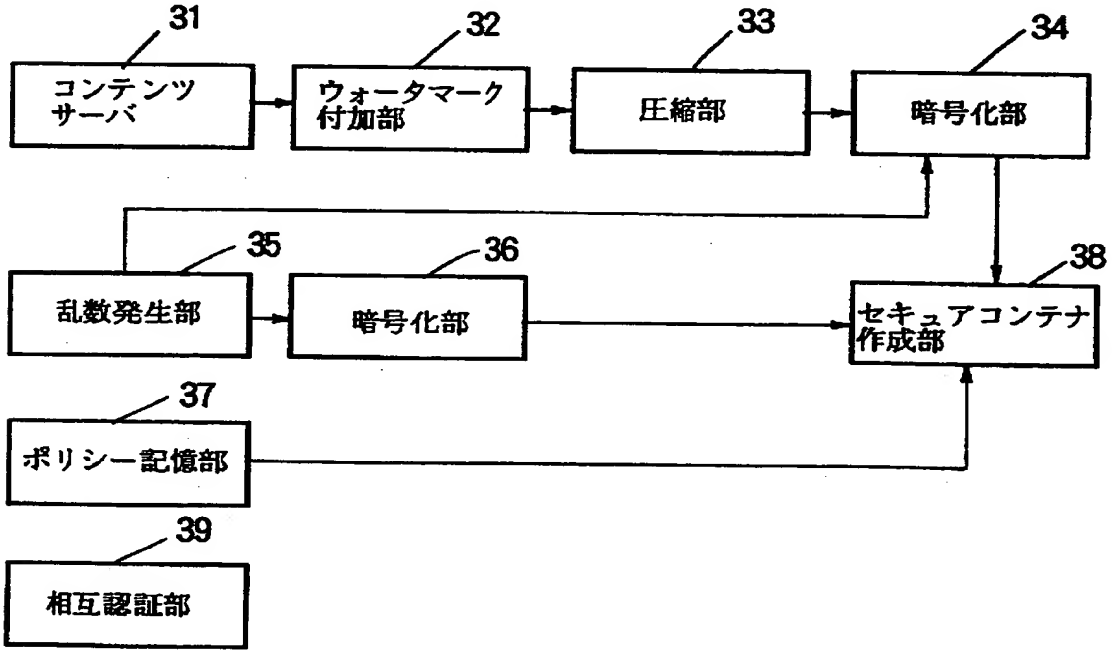
【図６】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
配送用鍵を送信
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

【図７】

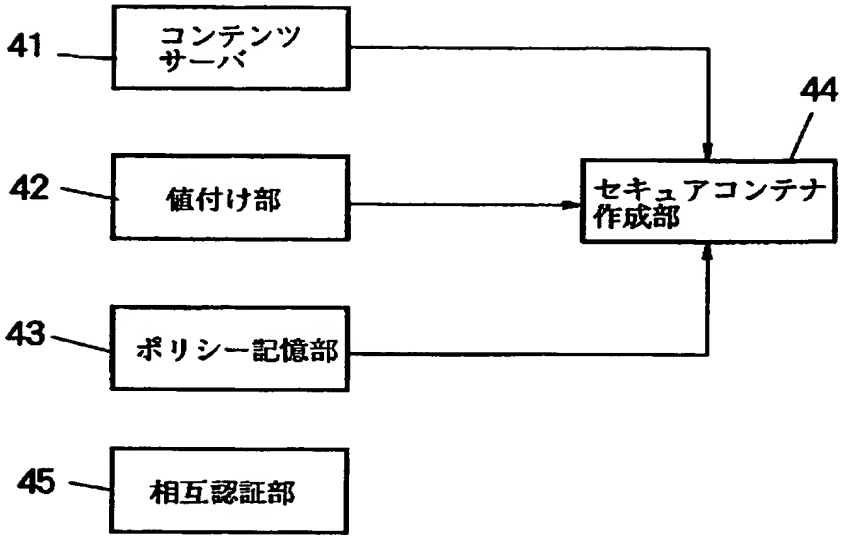
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
・・・			
FFFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFFh	不可	可	可

【図８】

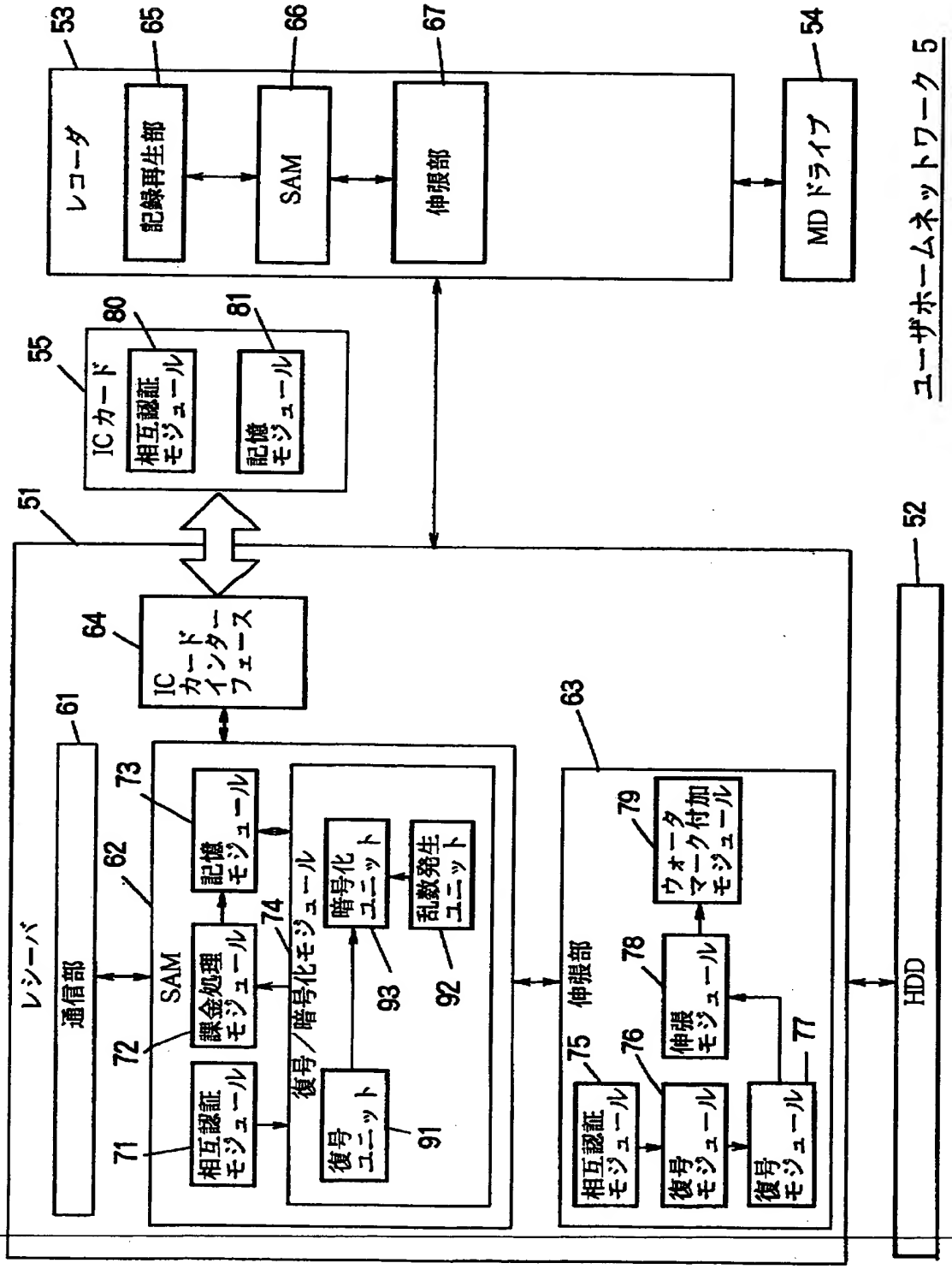


コンテンツプロバイダ 2

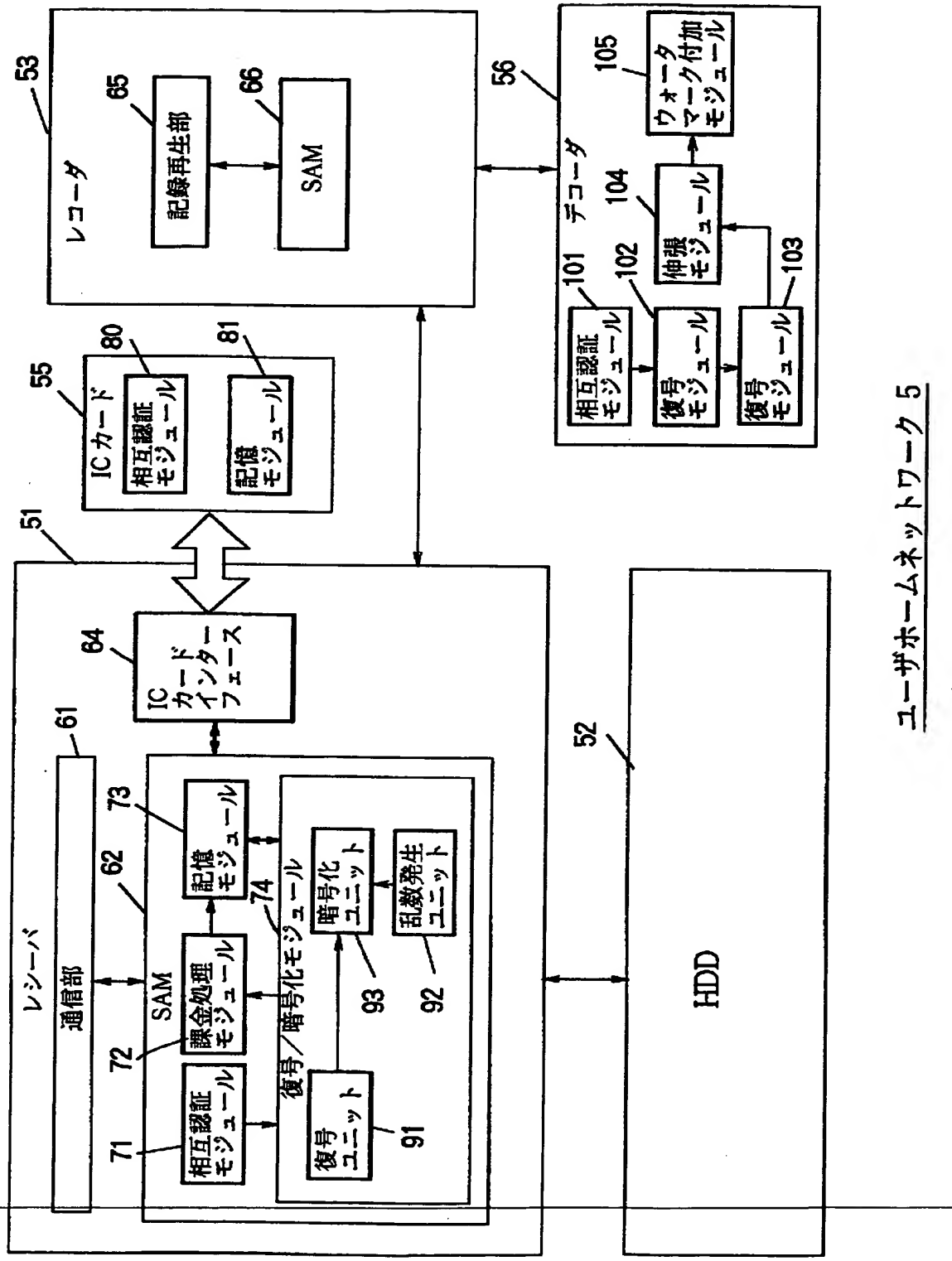
【図９】


41
コンテンツ
サーバ
44
42
値付け部
セキュアコンテナ
作成部
43
ポリシー記憶部
45
相互認証部
サービスプロバイダ 3

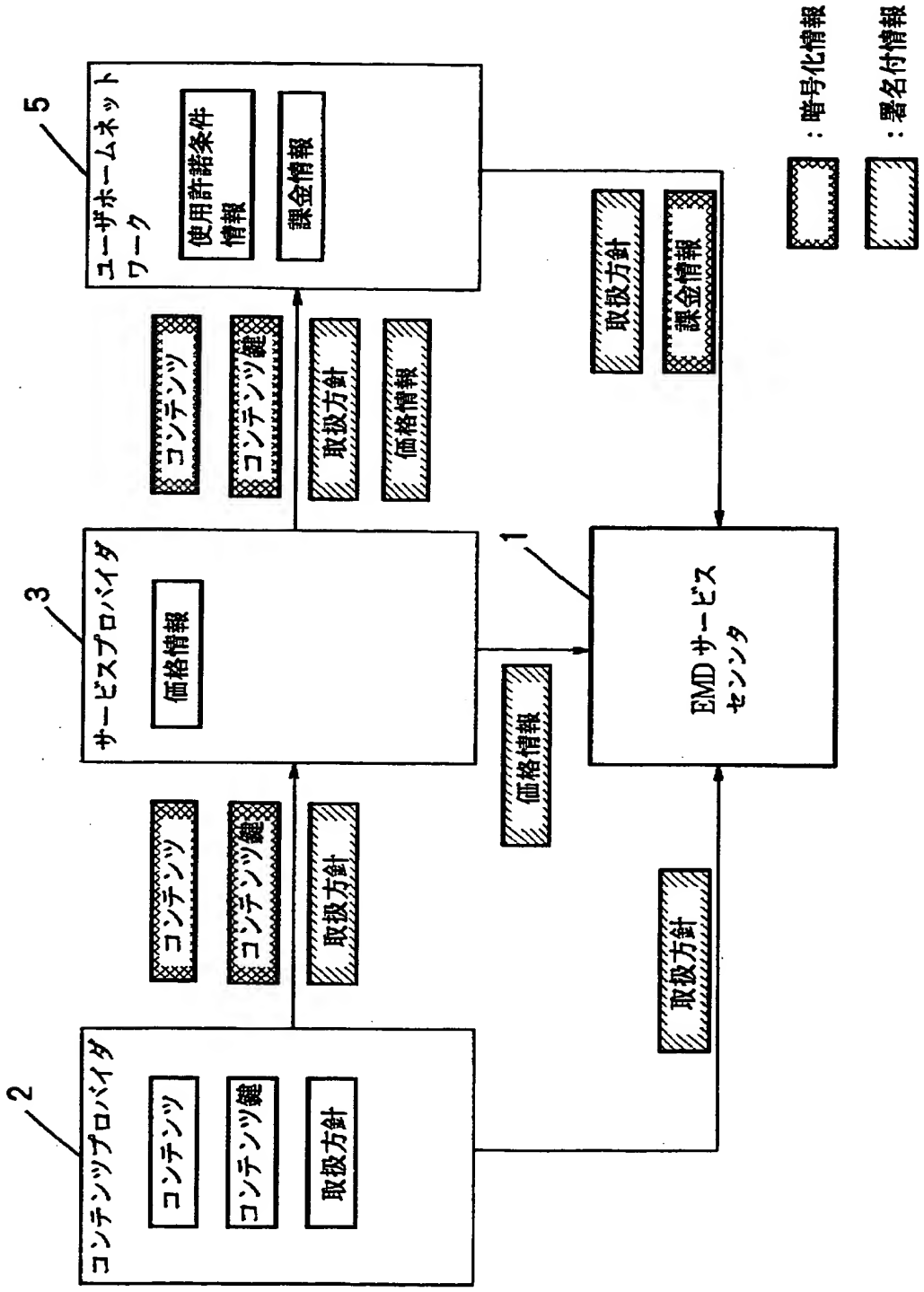
【図１０】


53
65
66
67
54
レコーダ
記録再生部
SAM
伸張部
MDドライブ
ユーザホームネットワーク 5
55
80
81
ICカード
相互認証モジュール
記憶モジュール
51
52
64
ICカードインターフェース
61
63
レシーバ
通信部
62
SAM
73
記憶モジュール
暗号化モジュール
暗号化ユニット
乱数発生ユニット
74
課金処理モジュール
72
相互認証モジュール
71
復号／暗号化モジュール
復号ユニット
91
93
92
伸張部
79
ウォータマーク付加モジュール
78
伸張モジュール
75
76
77
相互認証モジュール
復号モジュール
復号モジュール
HDD

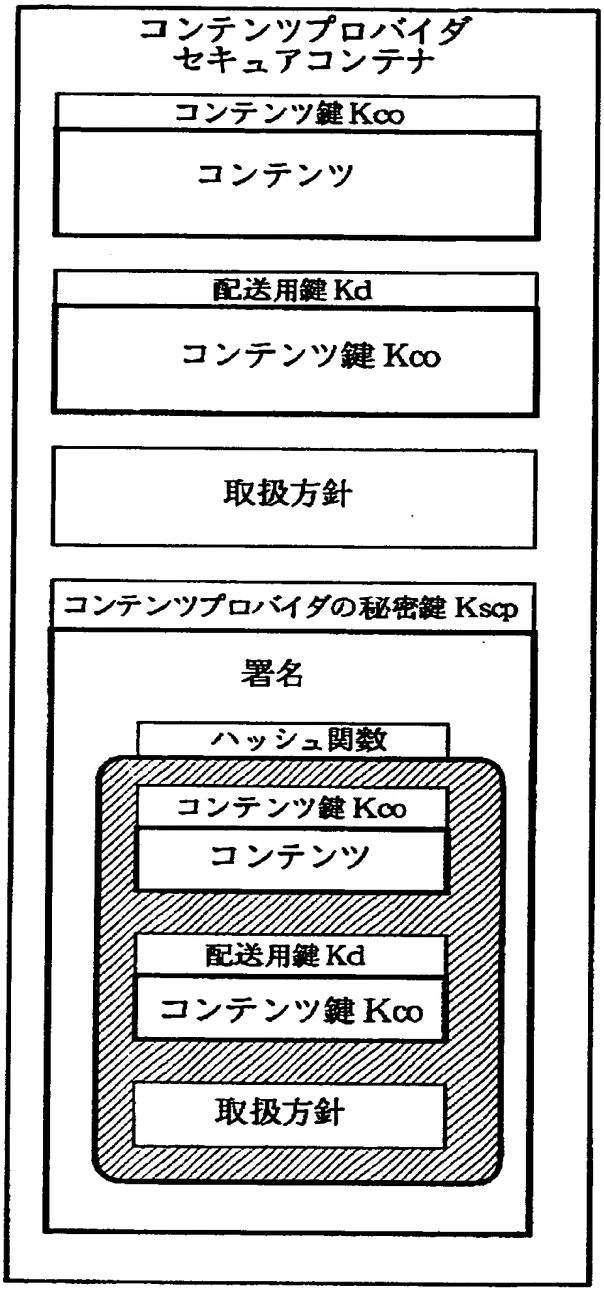
【図１１】


ユーザホームネットワーク 5
レコーダ
53
記録再生部
65
SAM
66
デコーダ
56
ウォータマーク付加モジュール
105
伸張モジュール
104
相互認証モジュール
101
復号モジュール
102
復号モジュール
103
ICカード
55
相互認証モジュール
80
記憶モジュール
81
51
ICカードインターフェース
64
レシーバ
61
通信部
62
SAM
相互認証モジュール
71
課金処理モジュール
72
記憶モジュール
73
復号/暗号化モジュール
74
復号ユニット
91
暗号化ユニット
93
乱数発生ユニット
92
HDD
52

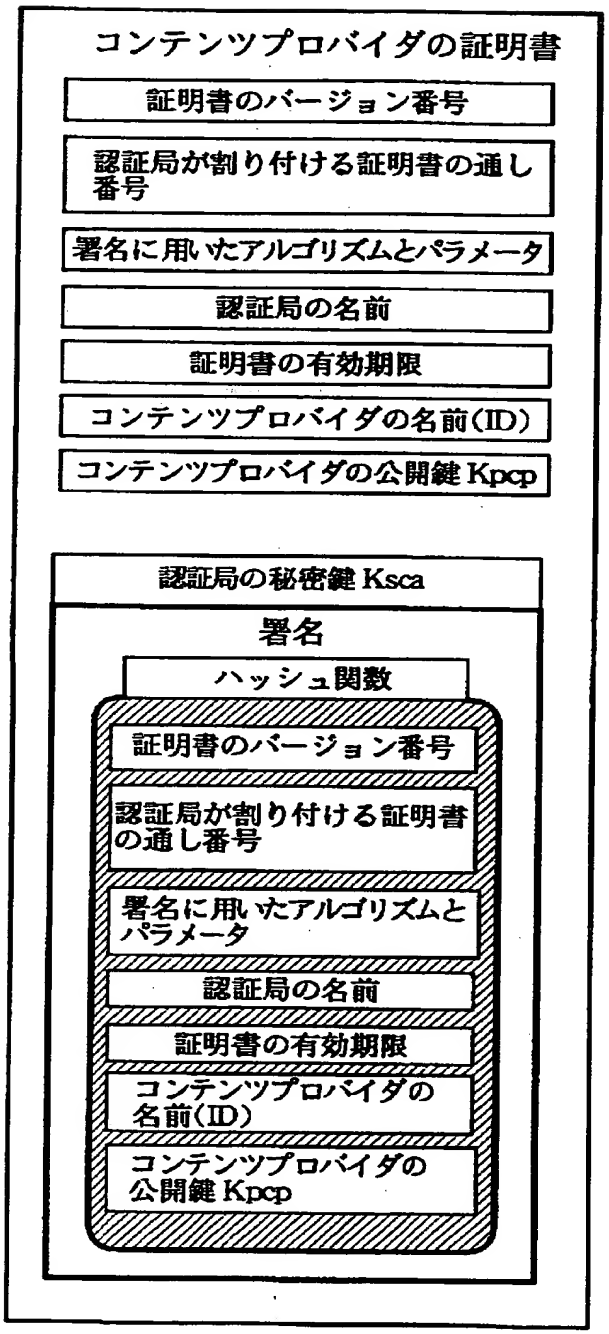
【図１２】


5
ユーザホームネットワーク
使用許諾条件情報
課金情報
3
サービスプロバイダ
価格情報
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
1
EMDサービスセンタ
コンテンツ
コンテンツ鍵
取扱方針
価格情報
取扱方針
課金情報
取扱方針
：暗号化情報
：署名付情報

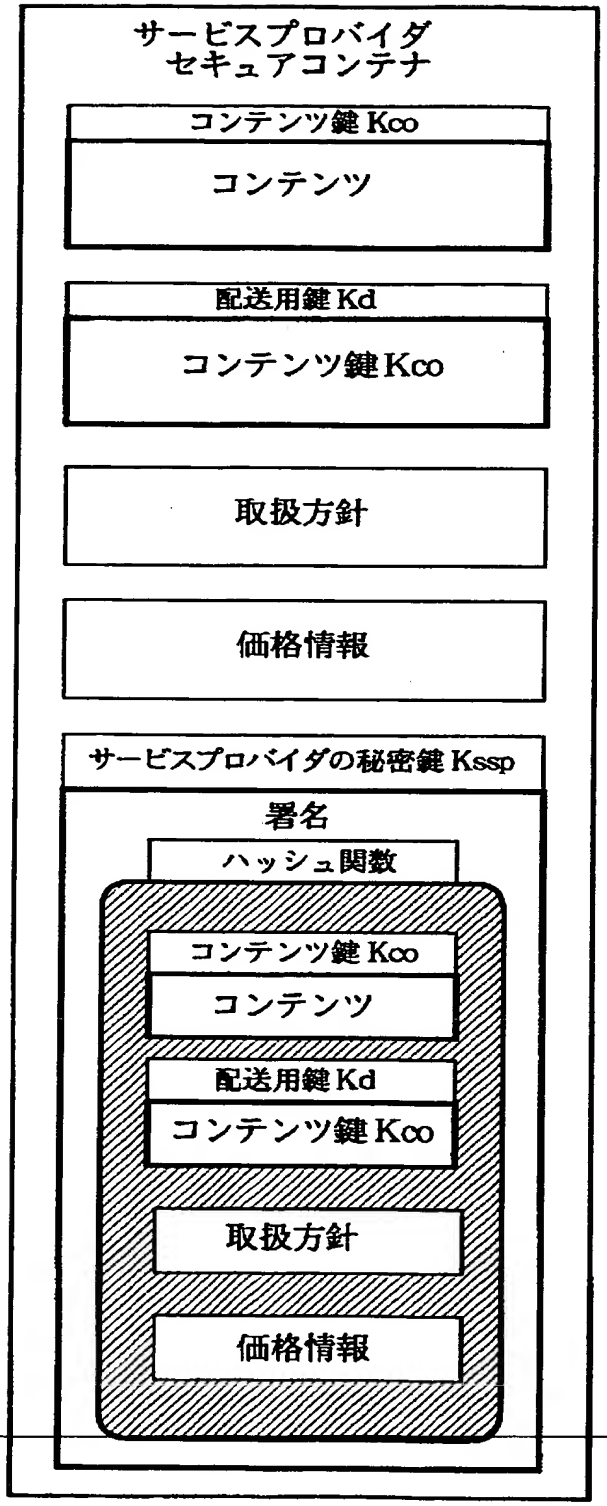
【図１３】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針

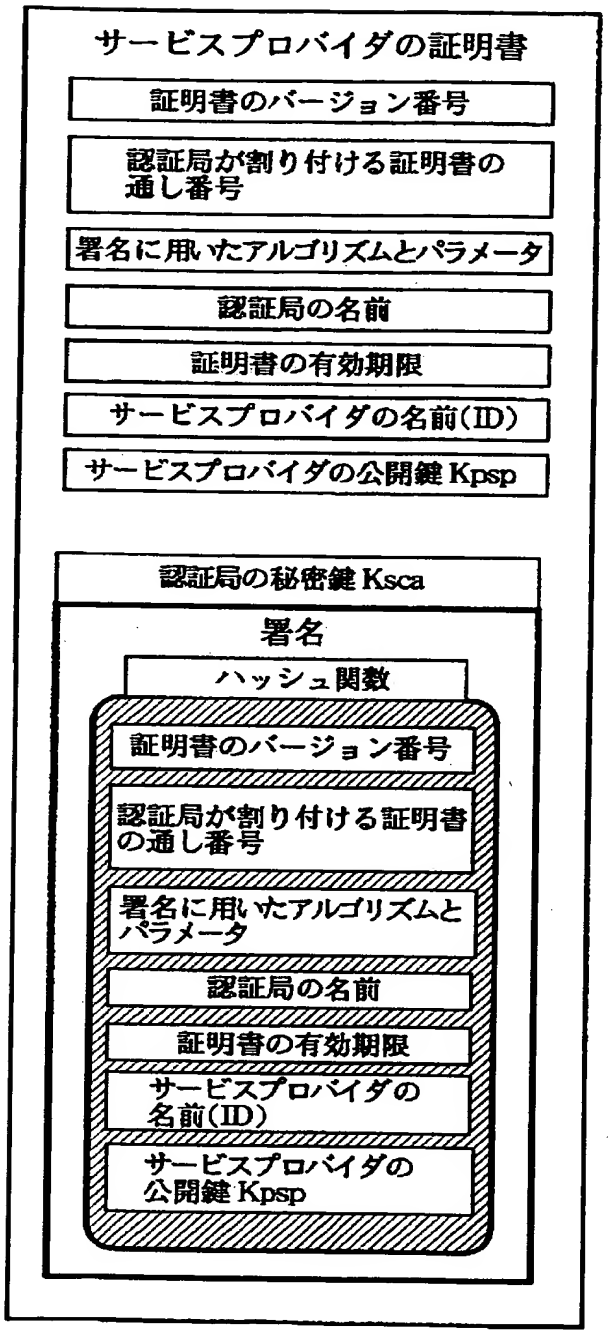
【図１４】


コンテンツプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp

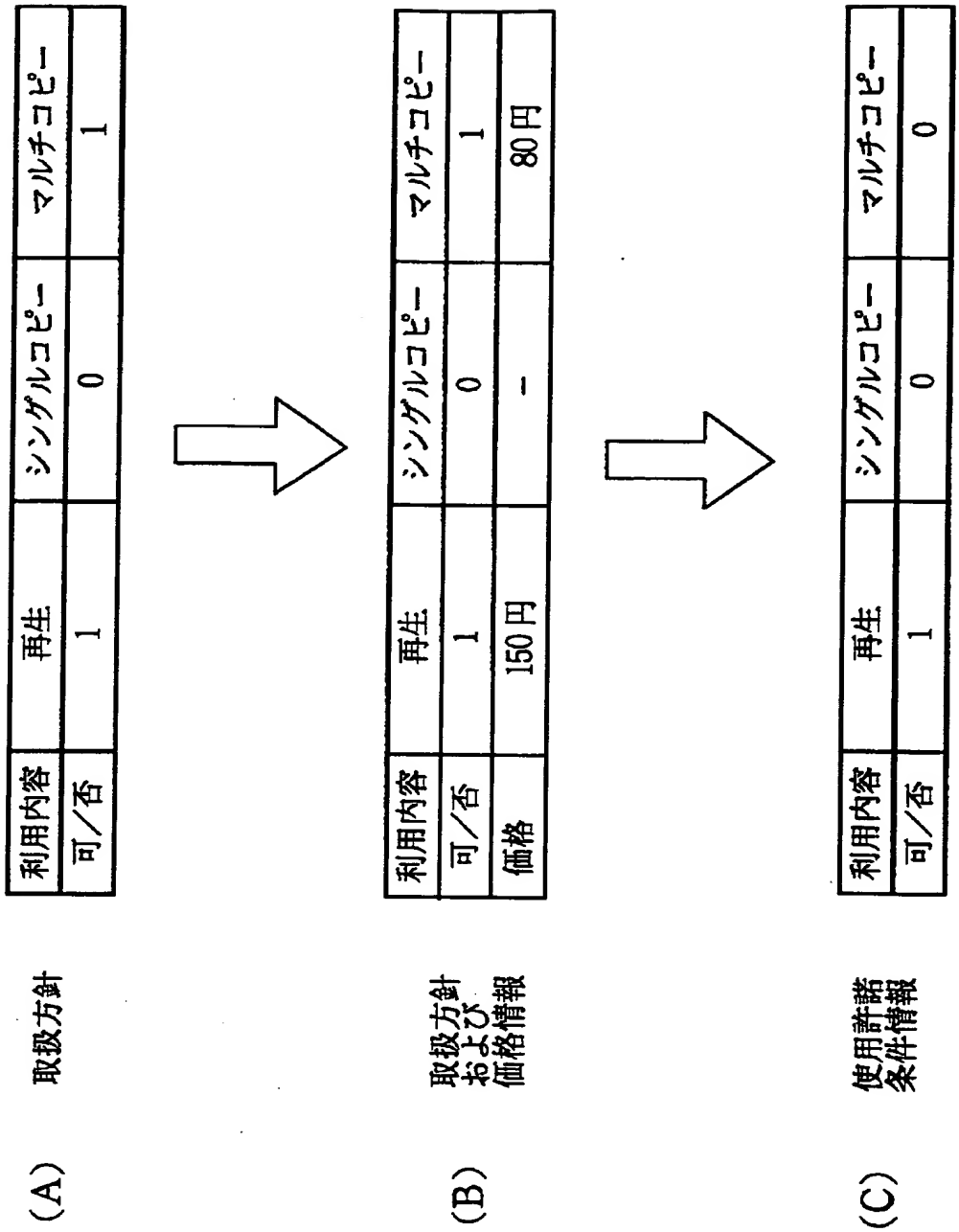
【図１５】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
価格情報

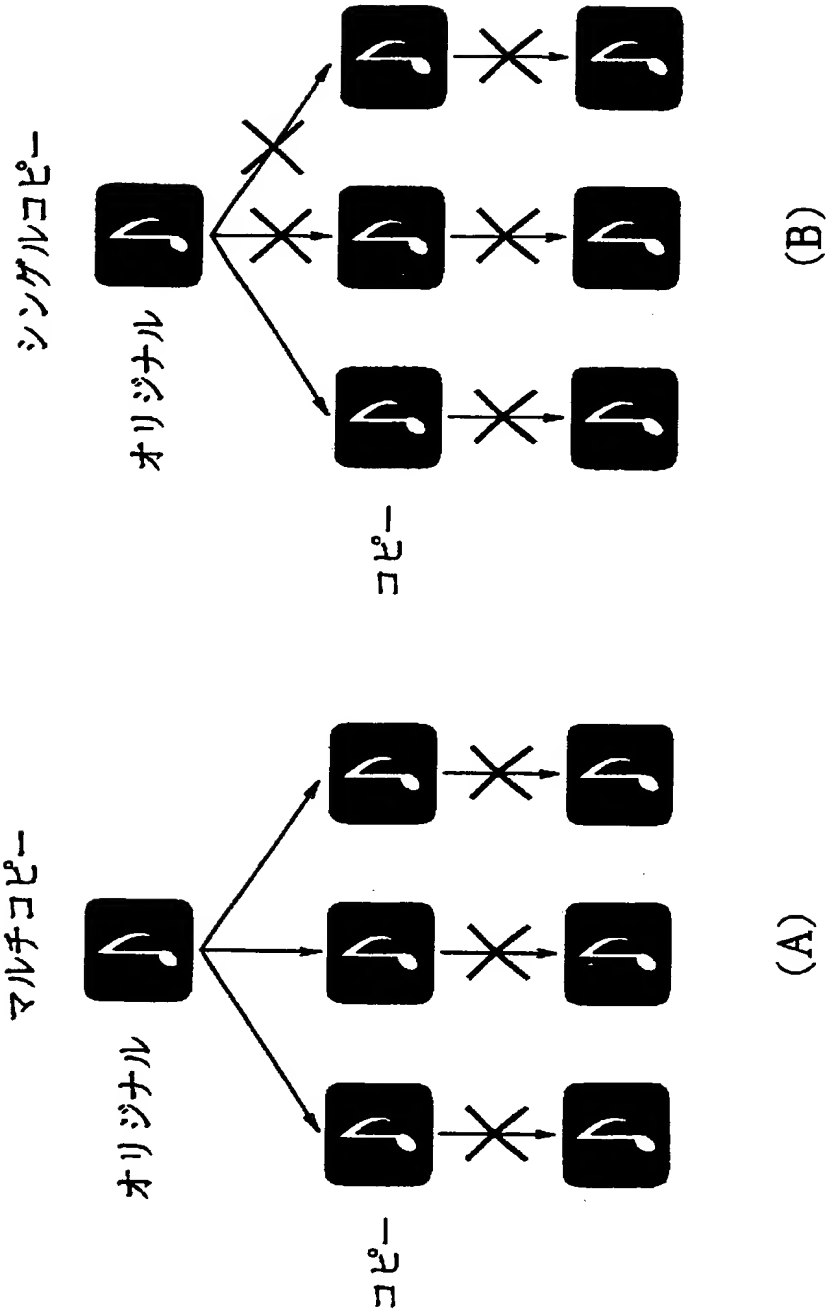
【図１６】


サービスプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp

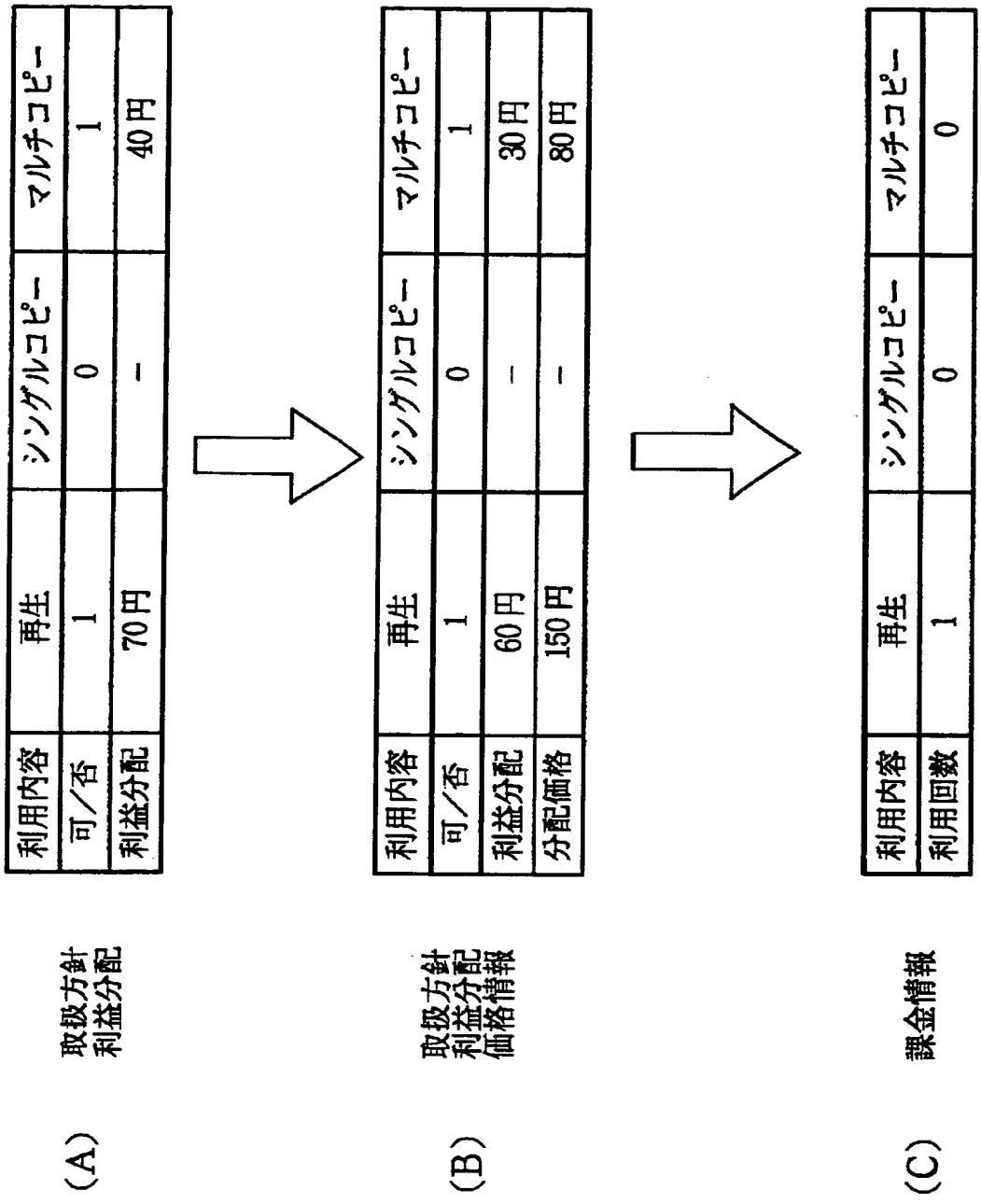
【図１７】


(A)
取扱方針
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
(B)
取扱方針
および
価格情報
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
価格
150円
－
80円
(C)
使用許諾
条件情報
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
0

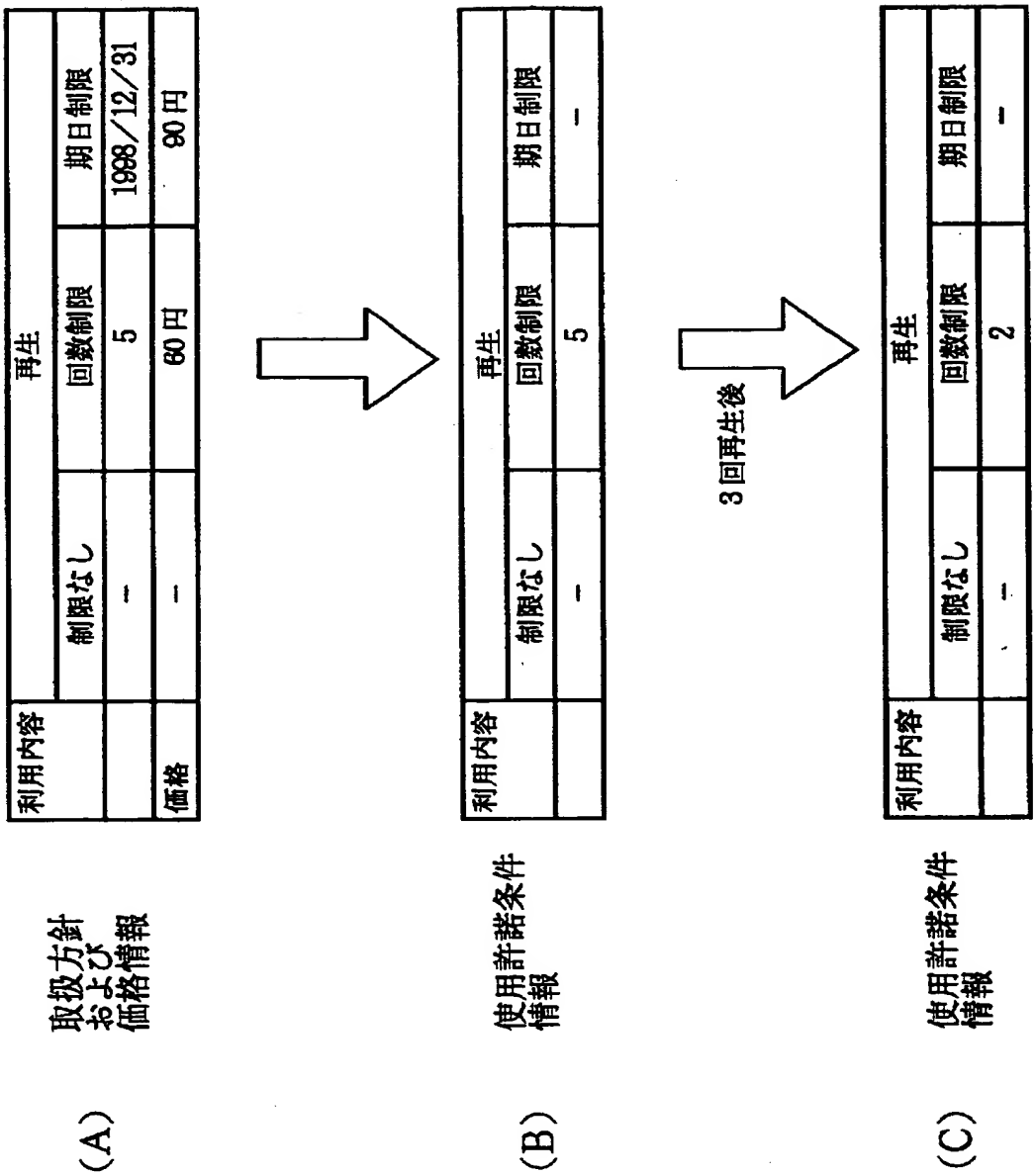
【図１８】



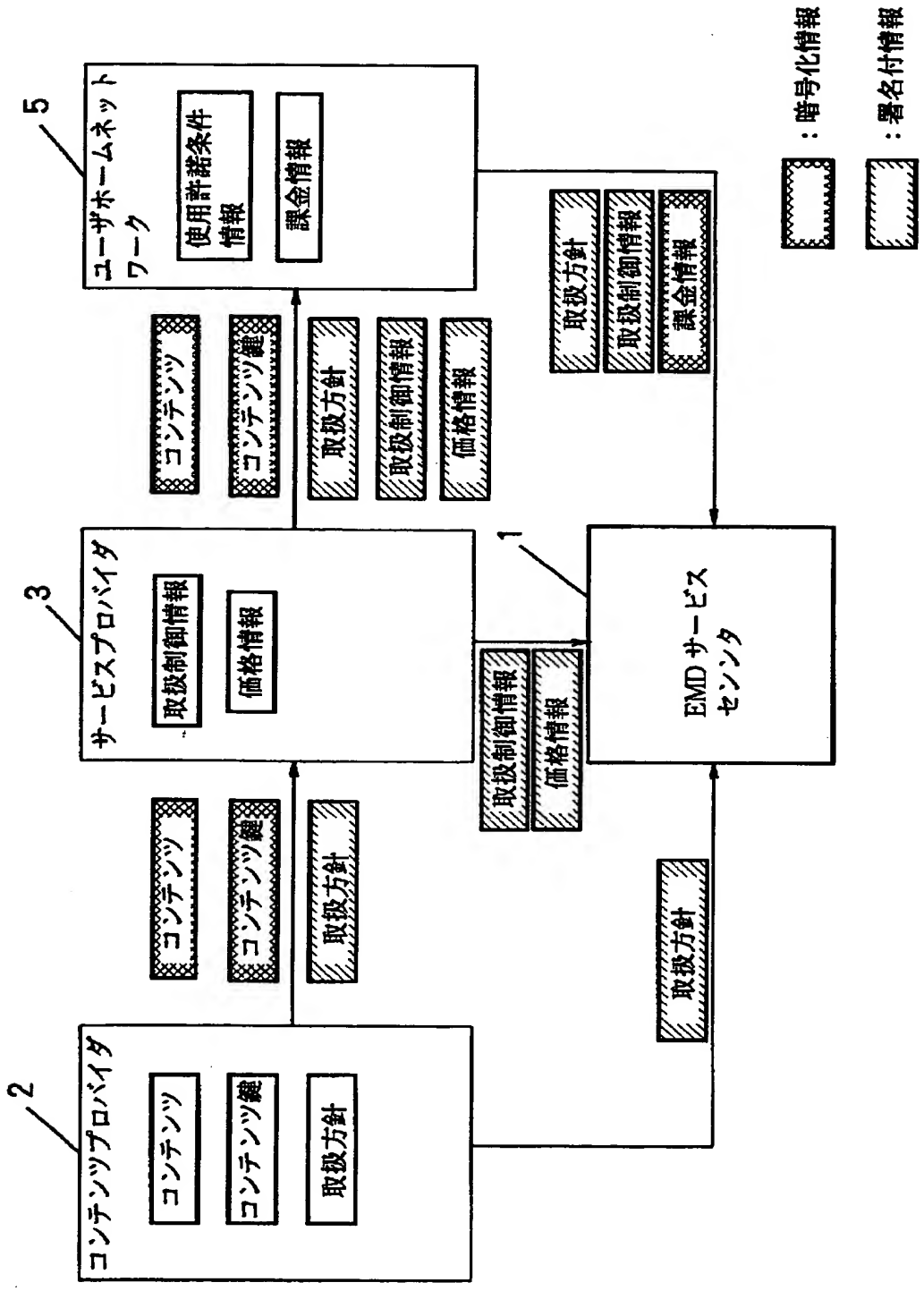
【図１９】


利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
利益分配
70円
－
40円
取扱方針
利益分配
(A)
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
利益分配
60円
－
30円
分配価格
150円
－
80円
取扱方針
利益分配
価格情報
(B)
利用内容
再生
シングルコピー
マルチコピー
利用回数
1
0
0
課金情報
(C)

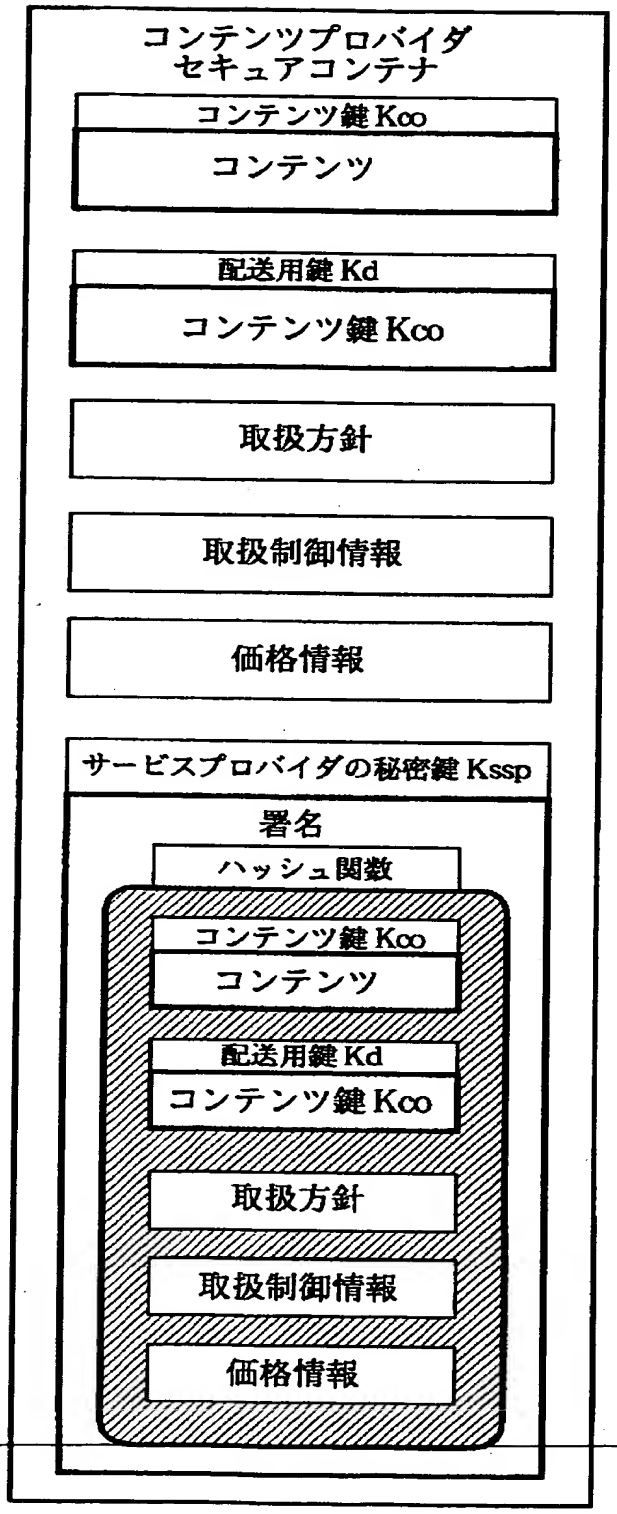
【図２０】


(A)
取扱方針および価格情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
1998／12／31
価格
－
60円
90円
(B)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
－
3回再生後
(C)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
2
－

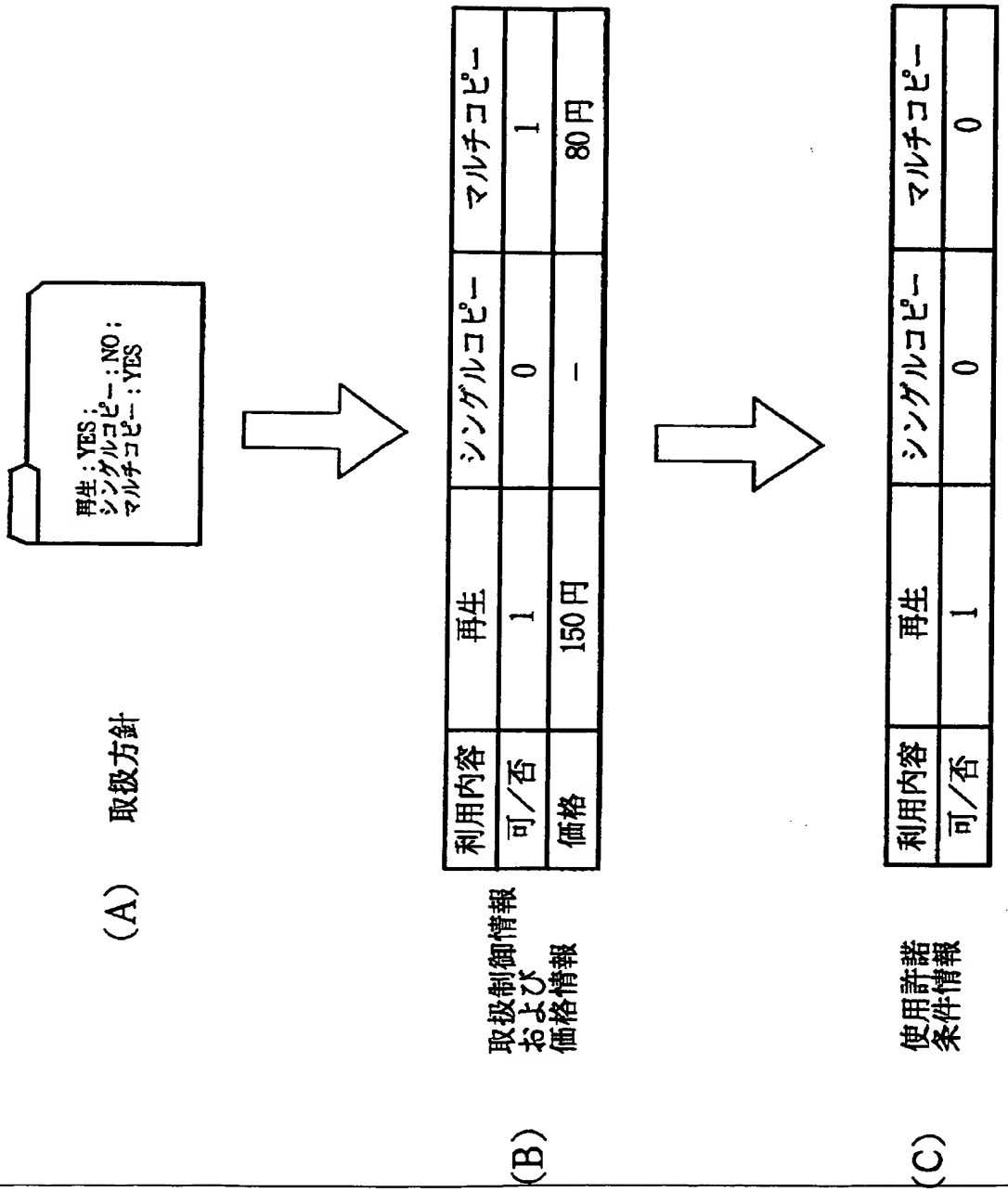
【図２１】


：暗号化情報
：署名付情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
1
EMD サービスセンタ
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針

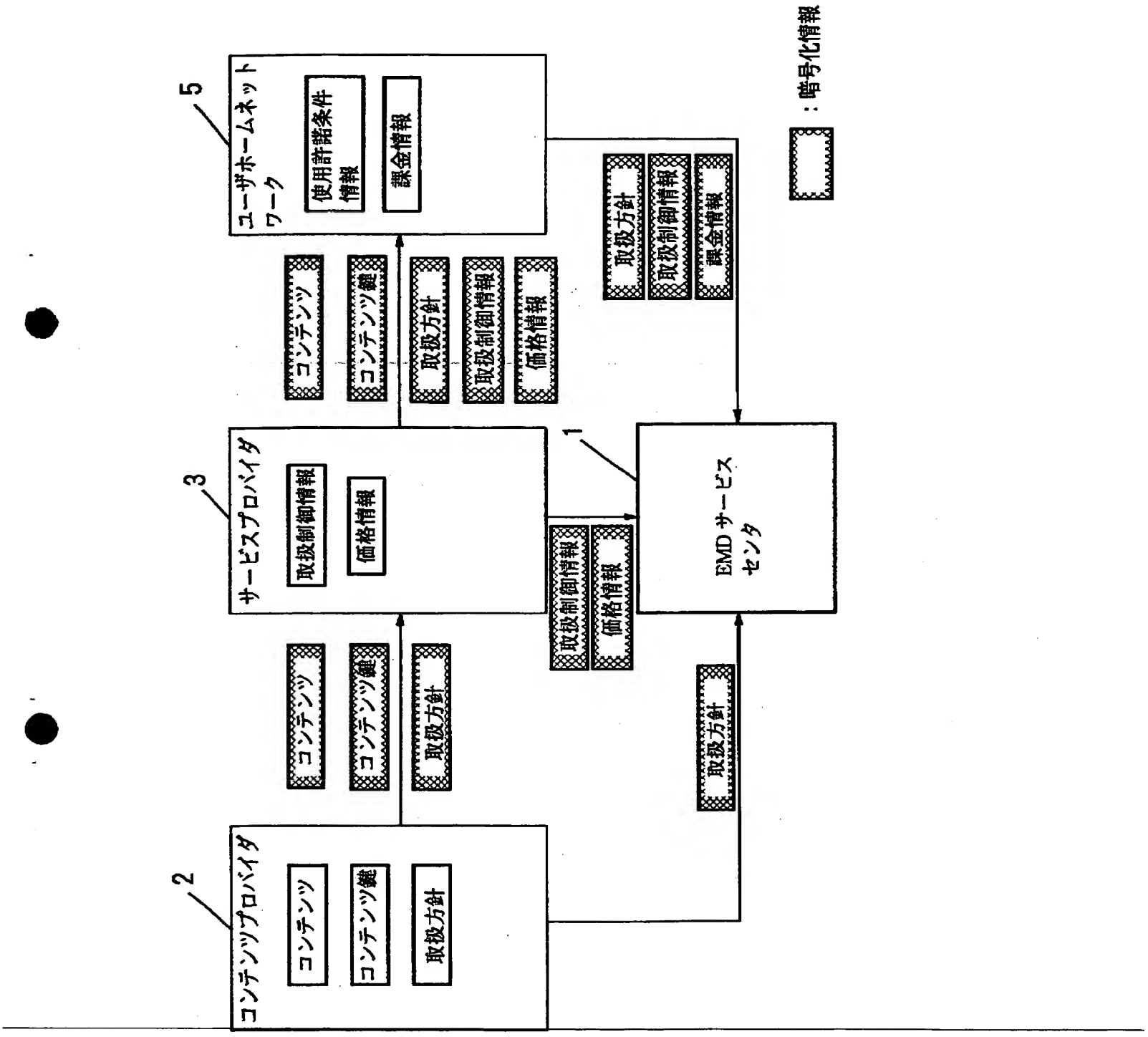
【図２２】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
取扱制御情報
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
取扱制御情報
価格情報

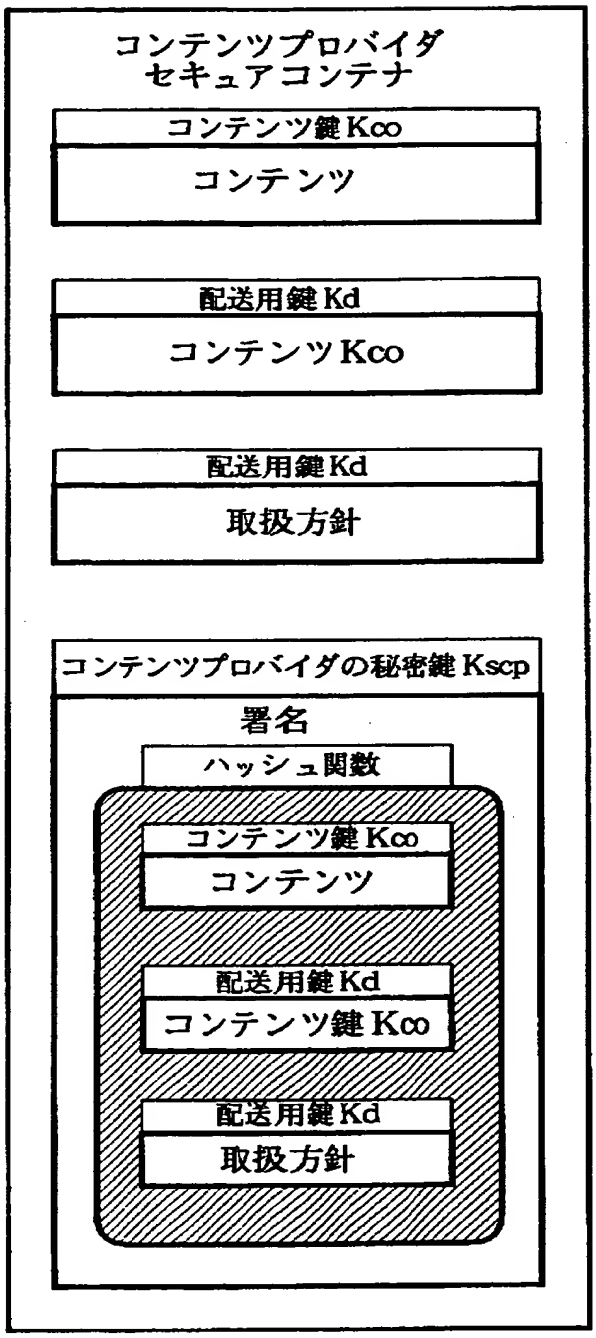
【図２３】


(A) 取扱方針
再生：YES；
シングルコピー：NO；
マルチコピー：YES
(B) 取扱制御情報および価格情報
利用内容
可／否
価格
再生
1
150円
シングルコピー
0
—
マルチコピー
1
80円
(C) 使用許諾条件情報
利用内容
可／否
再生
1
シングルコピー
0
マルチコピー
0

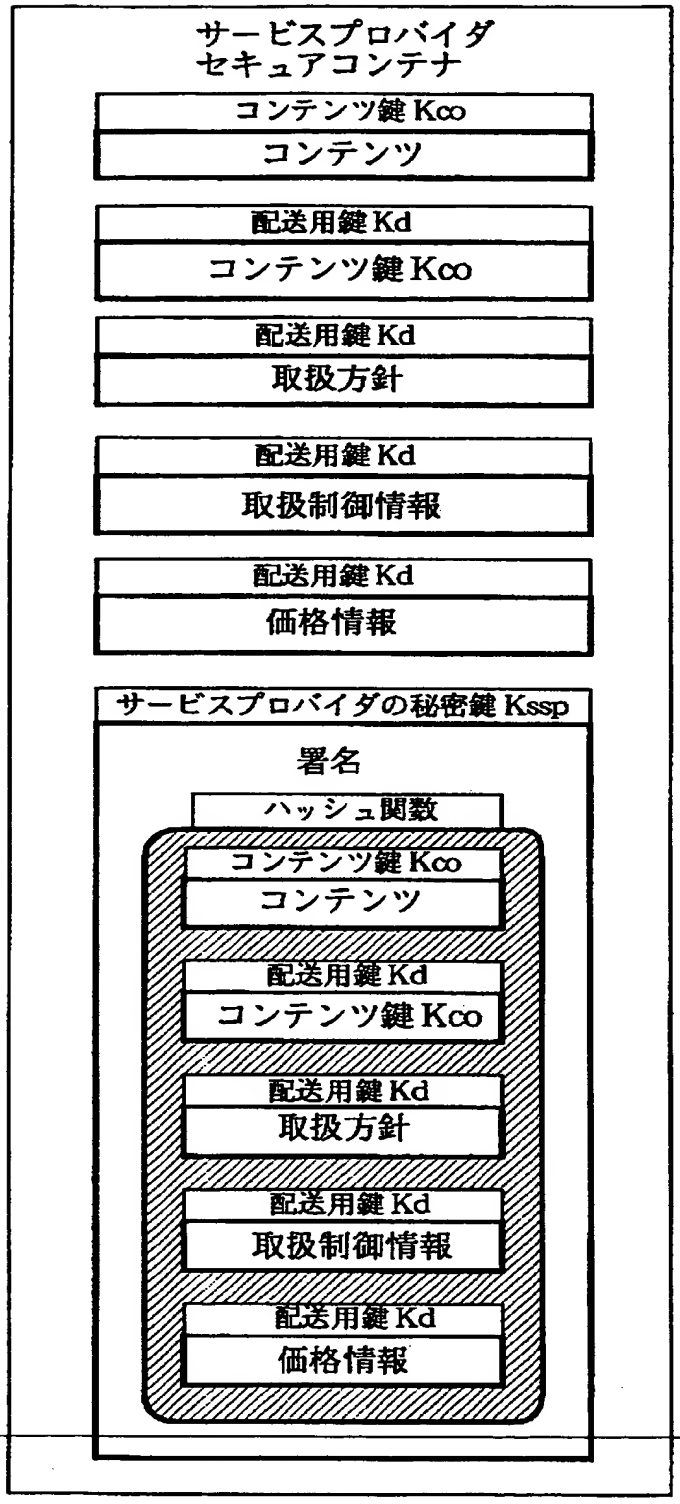
【図２４】


：暗号化情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
1
EMDサービスセンタ
取扱制御情報
価格情報
コンテンツ
コンテンツ鍵
取扱方針
取扱方針
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針

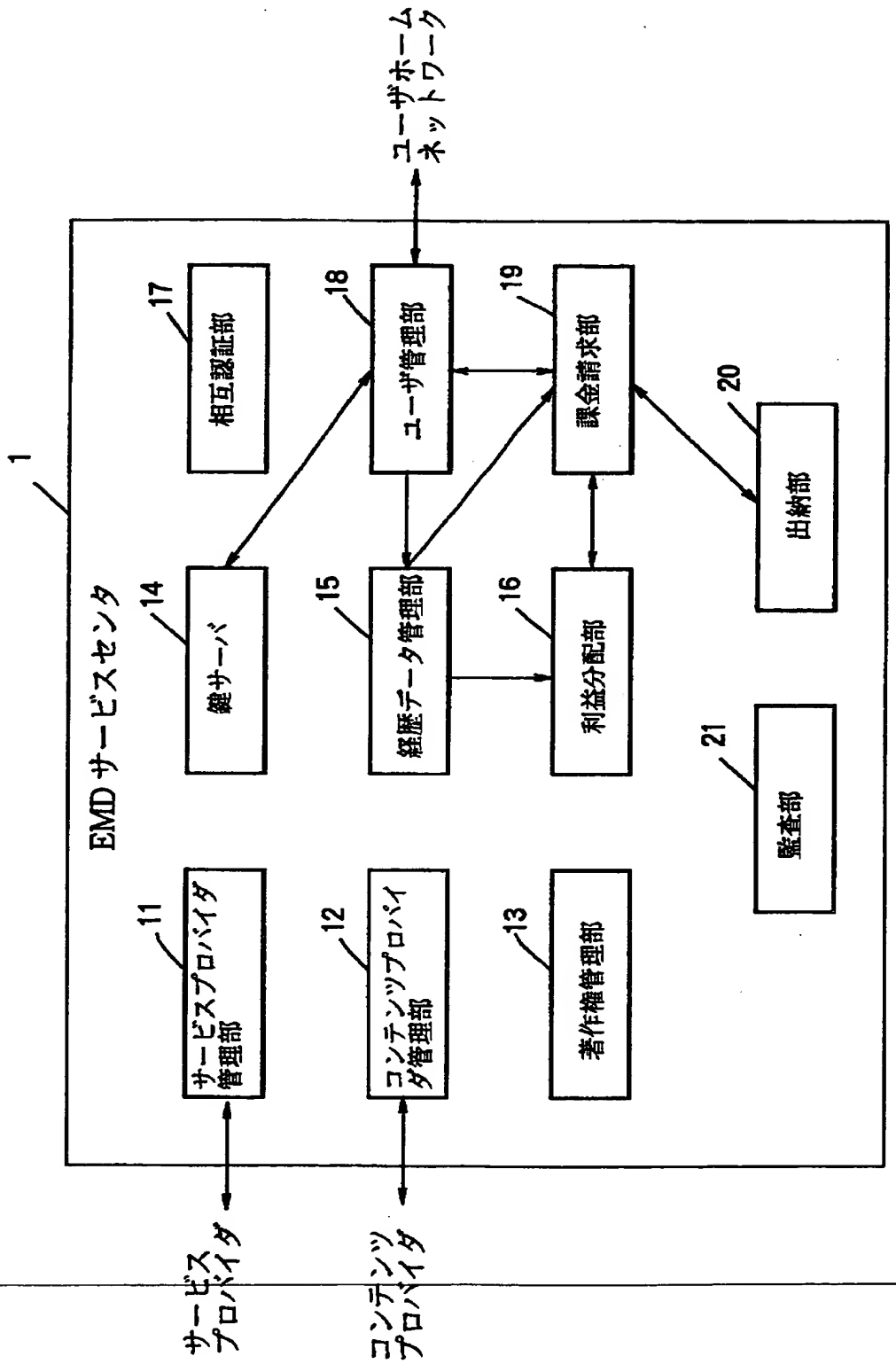
【図２５】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツKco
配送用鍵Kd
取扱方針
コンテンツプロバイダの秘密鍵Kscp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
配送用鍵Kd
取扱方針

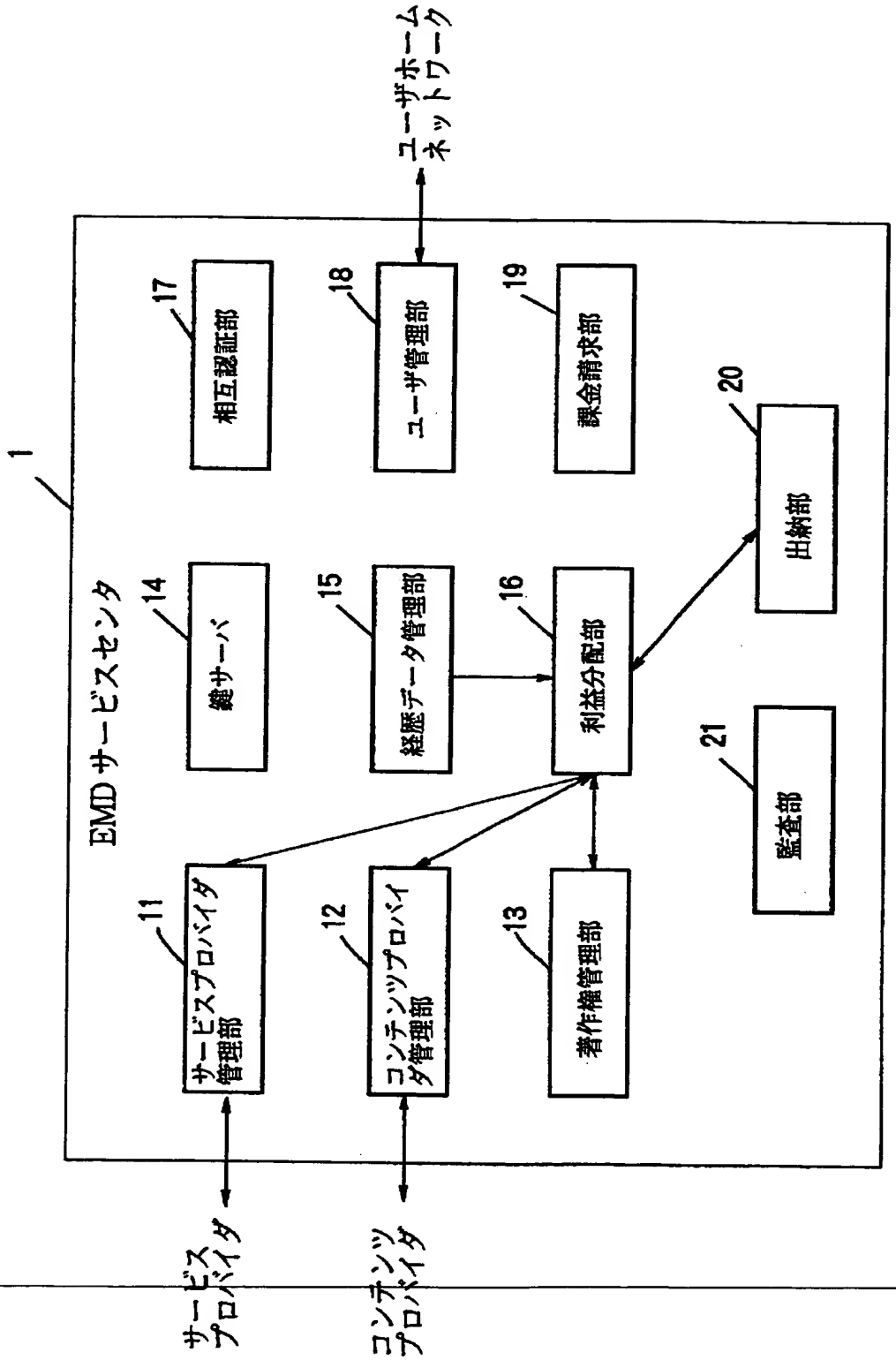
【図２６】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報

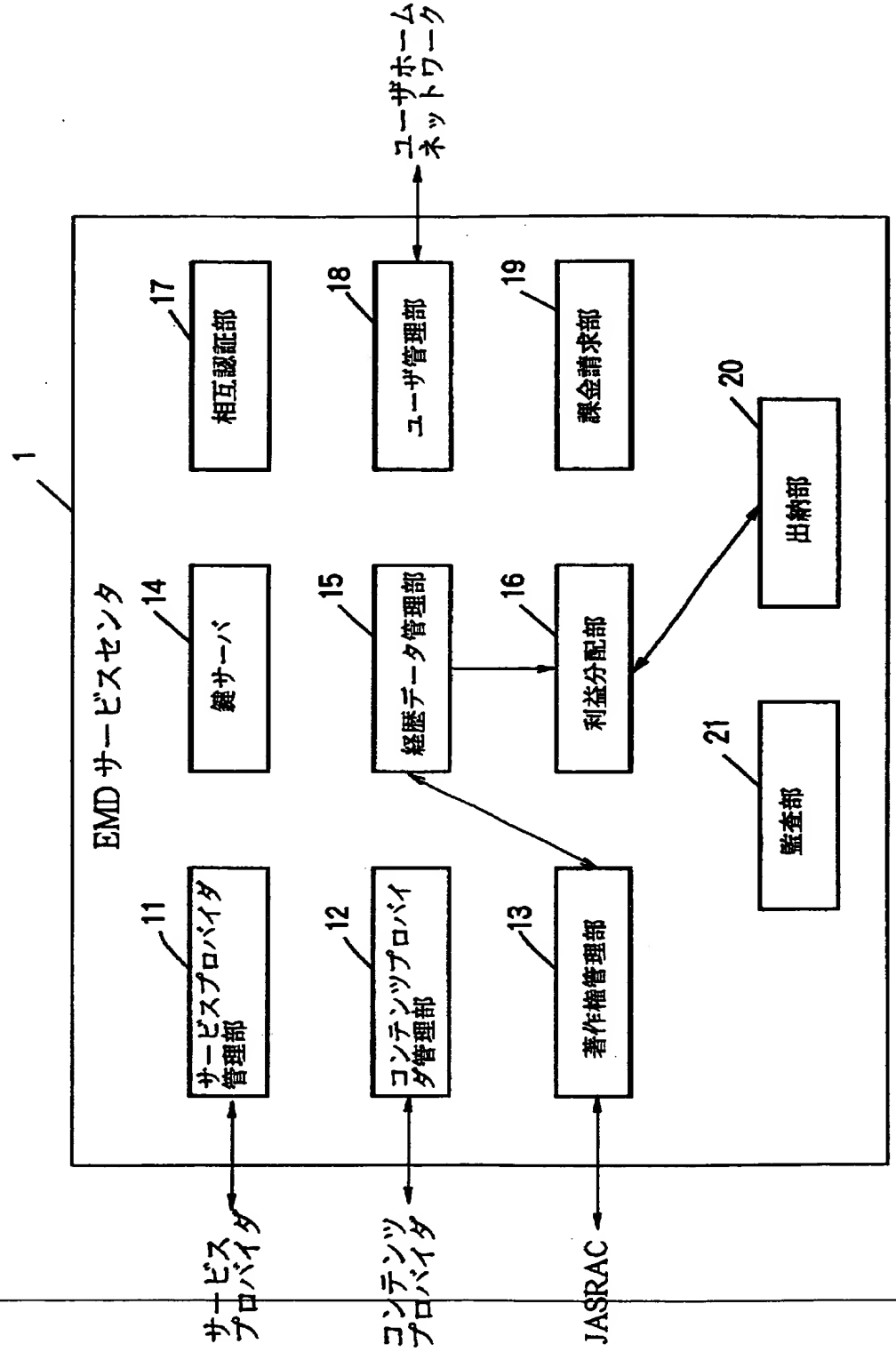
【図２７】


ユーザホームネットワーク
1
EMDサービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ

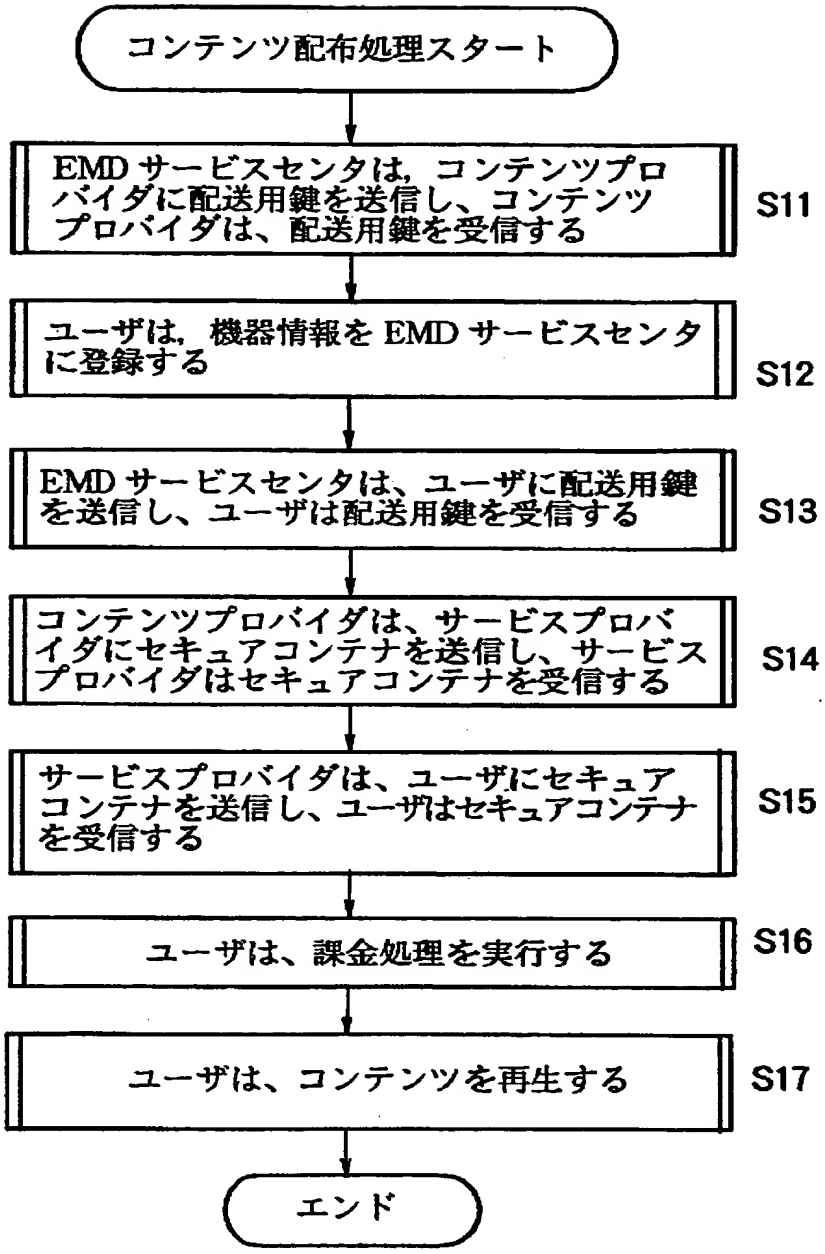
【図２８】


ユーザホームネットワーク
EMDサービスセンタ
1
相互認証部
17
ユーザ管理部
18
課金請求部
19
出納部
20
鍵サーバ
14
経歴データ管理部
15
利益分配部
16
監査部
21
サービスプロバイダ管理部
11
コンテンツプロバイダ管理部
12
著作権管理部
13
サービスプロバイダ
コンテンツプロバイダ

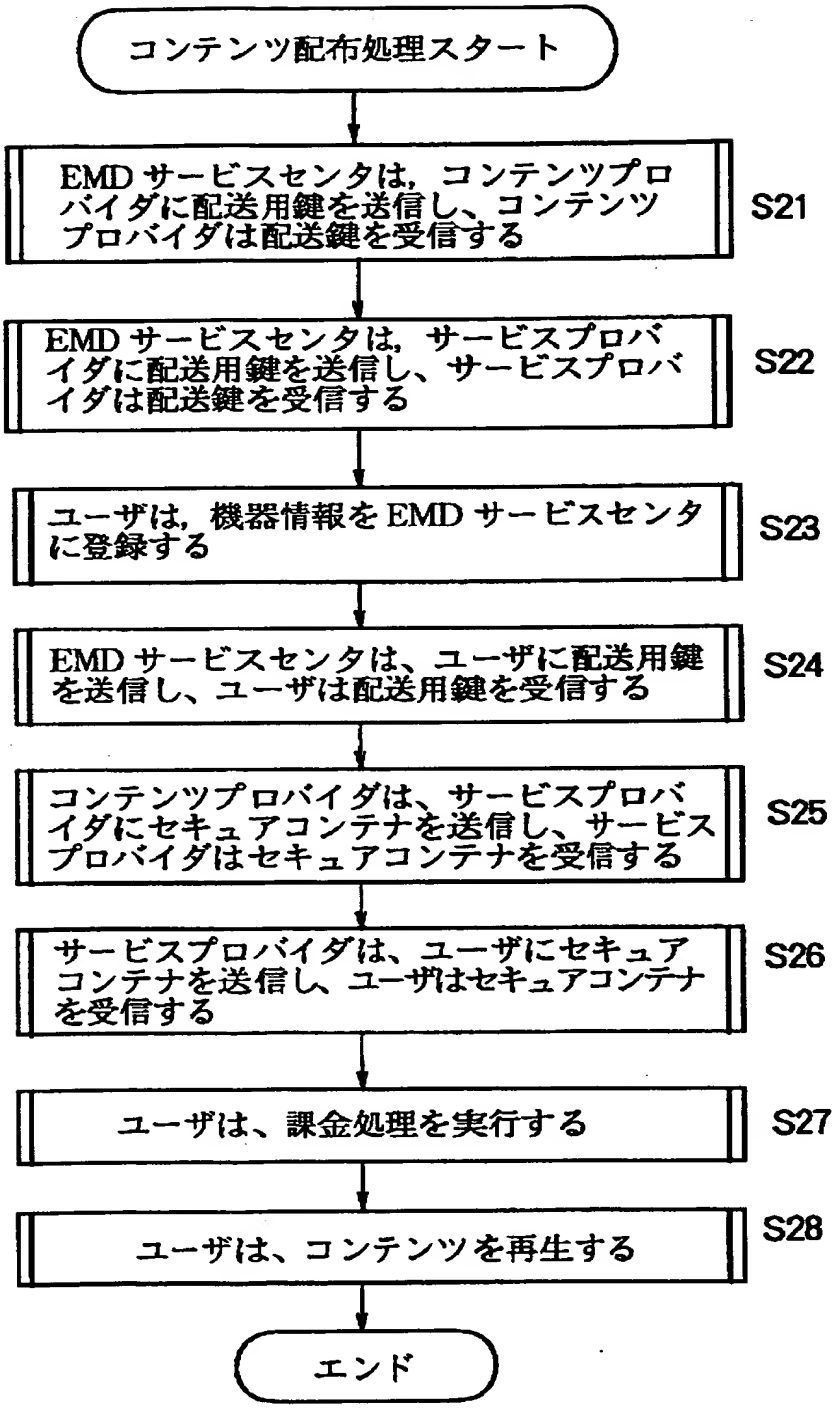
【図２９】


ユーザホームネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ
JASRAC

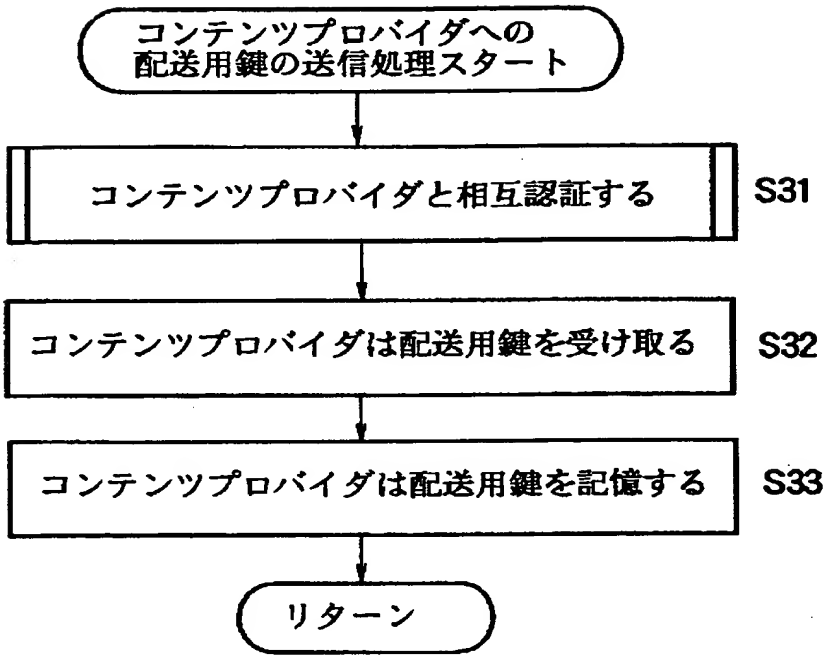
【図３０】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは，機器情報をEMDサービスセンタに登録する
S12
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド

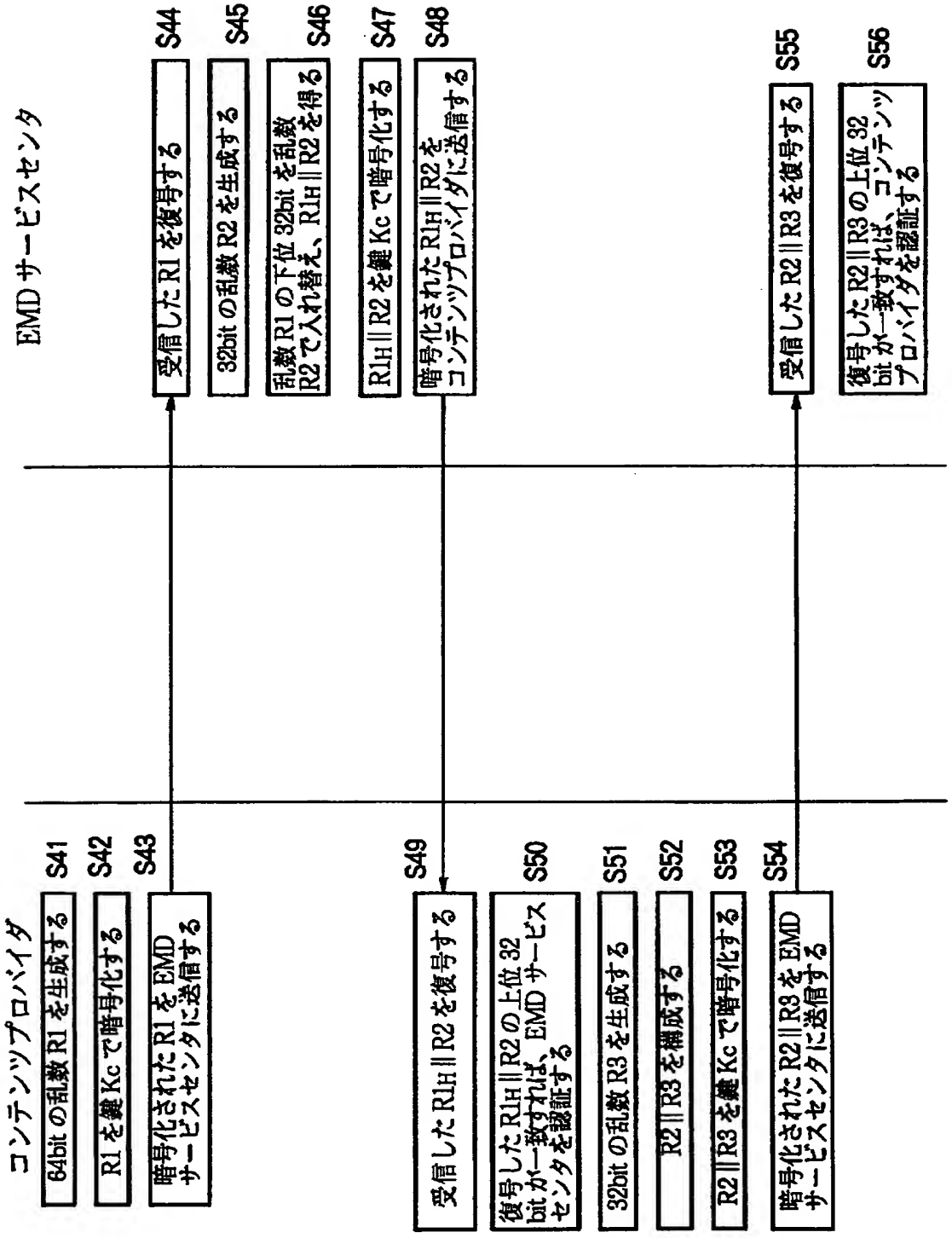
【図３１】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMDサービスセンタは，サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは，機器情報をEMDサービスセンタに登録する
S23
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド

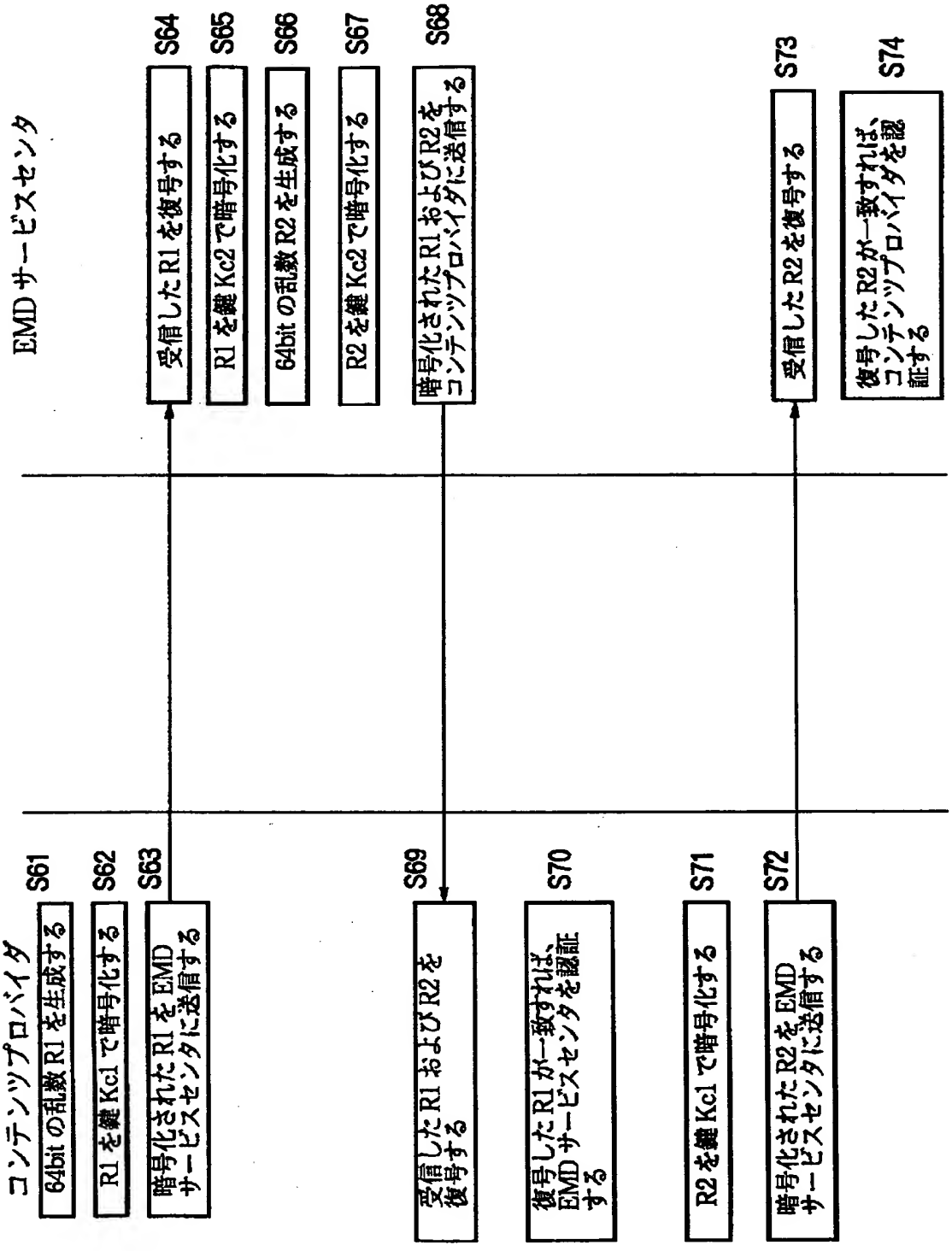
【図３２】


コンテンツプロバイダへの
配送用鍵の送信処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

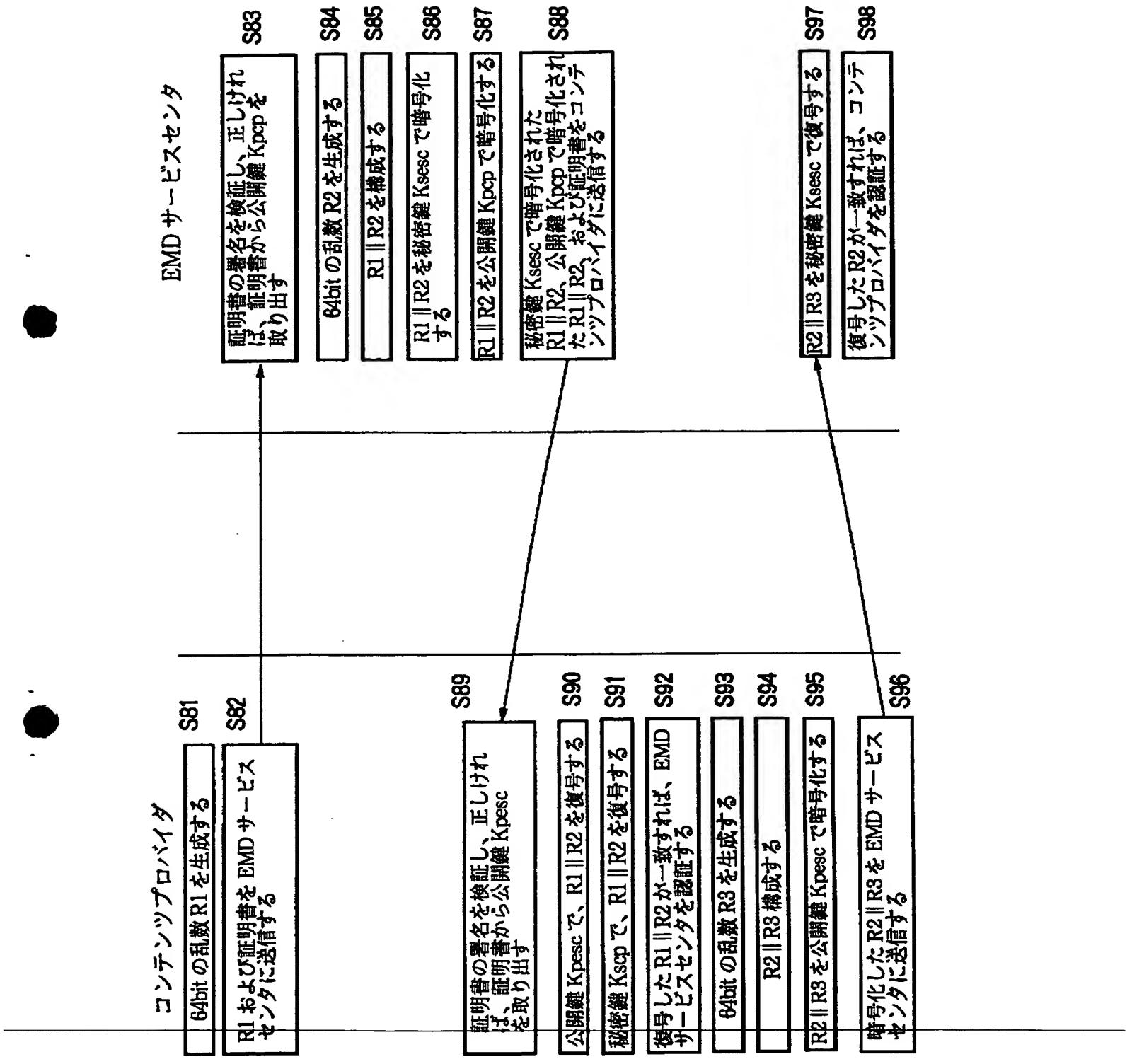
【図３３】


EMDサービスセンタ
コンテンツプロバイダ
S41
64bitの乱数R1を生成する
S42
R1を鍵Kcで暗号化する
S43
暗号化されたR1をEMDサービスセンタに送信する
S44
受信したR1を復号する
S45
32bitの乱数R2を生成する
S46
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S47
R1H||R2を鍵Kcで暗号化する
S48
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S49
受信したR1H||R2を復号する
S50
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S51
32bitの乱数R3を生成する
S52
R2||R3を構成する
S53
R2||R3を鍵Kcで暗号化する
S54
暗号化されたR2||R3をEMDサービスセンタに送信する
S55
受信したR2||R3を復号する
S56
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する

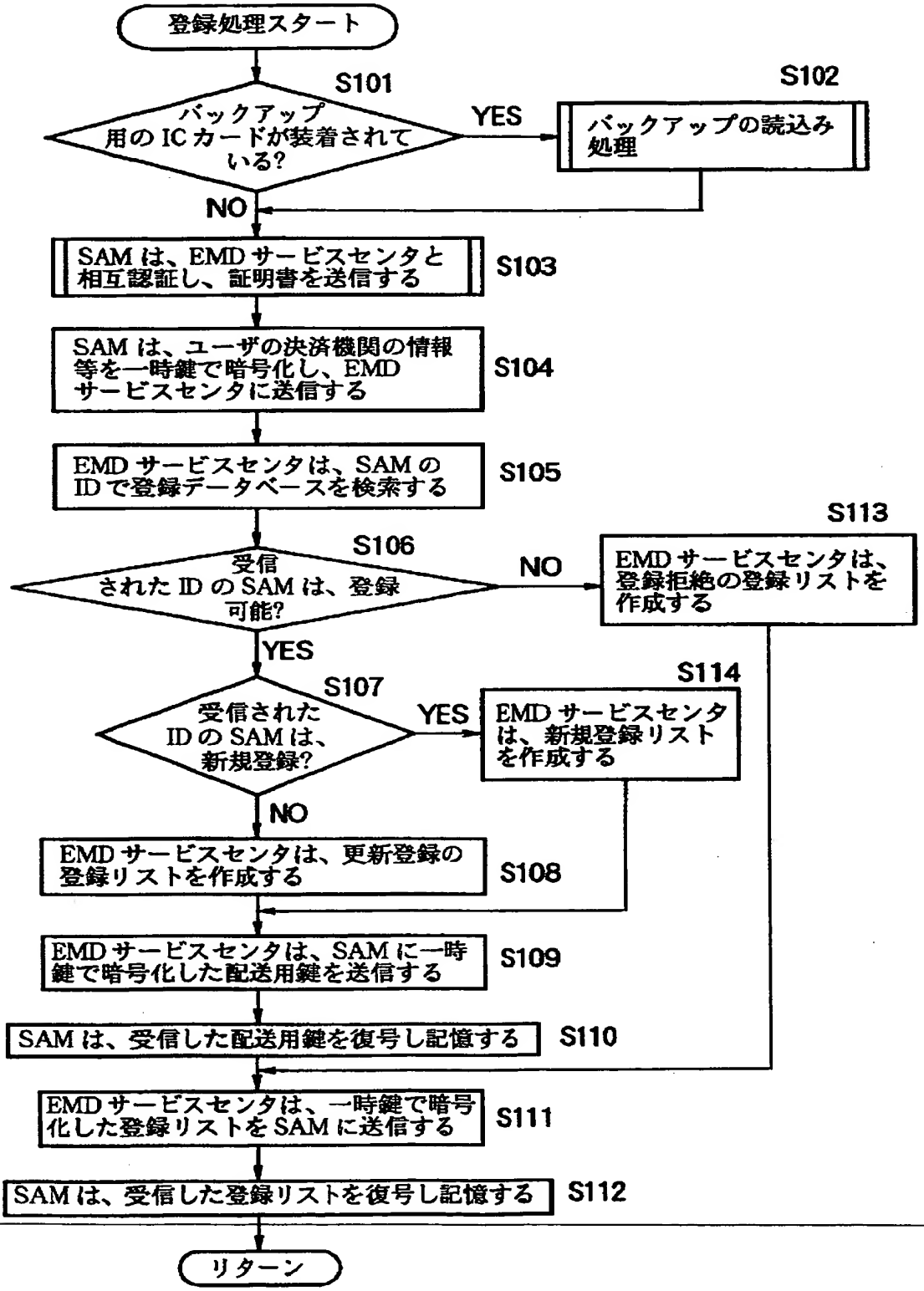
【図３４】


EMDサービスセンタ
コンテンツプロバイダ
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

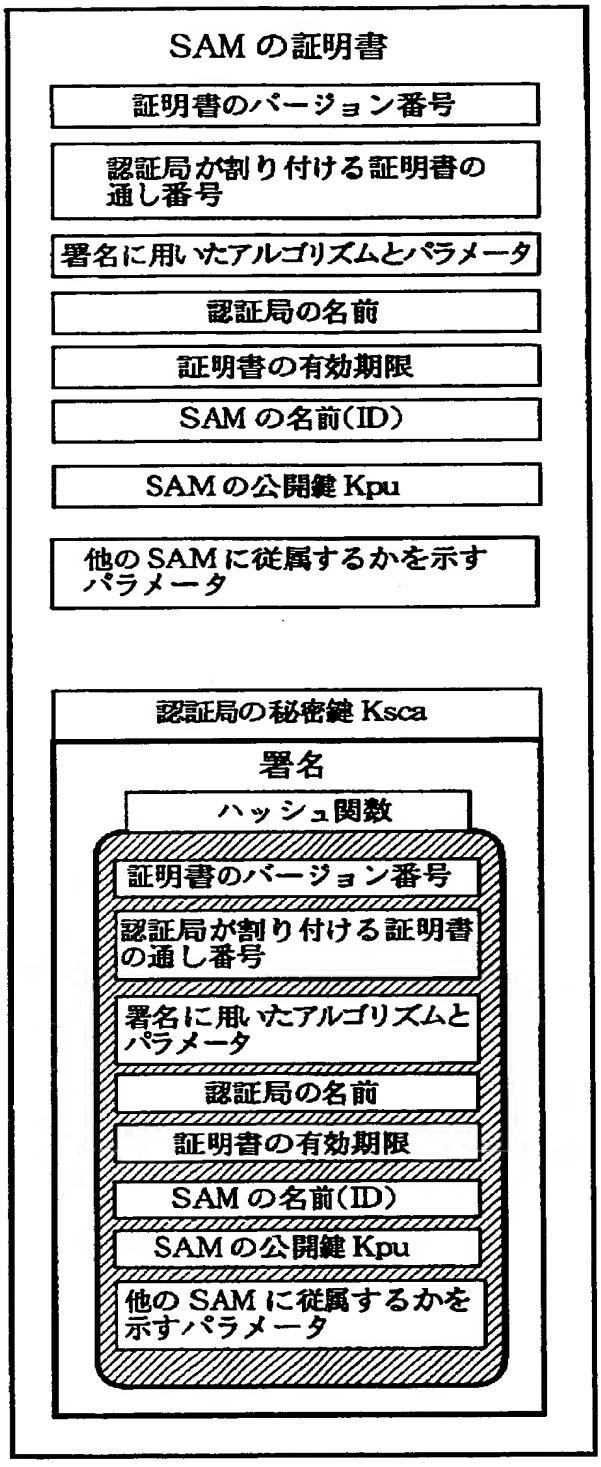
【図３５】


EMDサービスセンタ
コンテンツプロバイダ
S81
64bitの乱数R1を生成する
S82
R1および証明書をEMDサービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵Kpcpを取り出す
S84
64bitの乱数R2を生成する
S85
R1‖R2を構成する
S86
R1‖R2を秘密鍵Ksescで暗号化する
S87
R1‖R2を公開鍵Kpcpで暗号化する
S88
秘密鍵Ksescで暗号化されたR1‖R2、公開鍵Kpcpで暗号化されたR1‖R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵Kpescを取り出す
S90
公開鍵Kpescで、R1‖R2を復号する
S91
秘密鍵Kscpで、R1‖R2を復号する
S92
復号したR1‖R2が一致すれば、EMDサービスセンタを認証する
S93
64bitの乱数R3を生成する
S94
R2‖R3を構成する
S95
R2‖R3を公開鍵Kpescで暗号化する
S96
暗号化したR2‖R3をEMDサービスセンタに送信する
S97
R2‖R3を秘密鍵Ksescで復号する
S98
復号したR2が一致すれば、コンテンツプロバイダを認証する

【図３６】


登録処理スタート
S101
バックアップ用のICカードが装着されている?
YES
S102
バックアップの読込み処理
NO
SAMは、EMDサービスセンタと相互認証し、証明書を送信する
S103
SAMは、ユーザの決済機関の情報等を一時鍵で暗号化し、EMDサービスセンタに送信する
S104
EMDサービスセンタは、SAMのIDで登録データベースを検索する
S105
S106
受信されたIDのSAMは、登録可能?
NO
S113
EMDサービスセンタは、登録拒絶の登録リストを作成する
YES
S107
受信されたIDのSAMは、新規登録?
YES
S114
EMDサービスセンタは、新規登録リストを作成する
NO
EMDサービスセンタは、更新登録の登録リストを作成する
S108
EMDサービスセンタは、SAMに一時鍵で暗号化した配送用鍵を送信する
S109
SAMは、受信した配送用鍵を復号し記憶する
S110
EMDサービスセンタは、一時鍵で暗号化した登録リストをSAMに送信する
S111
SAMは、受信した登録リストを復号し記憶する
S112
リターン

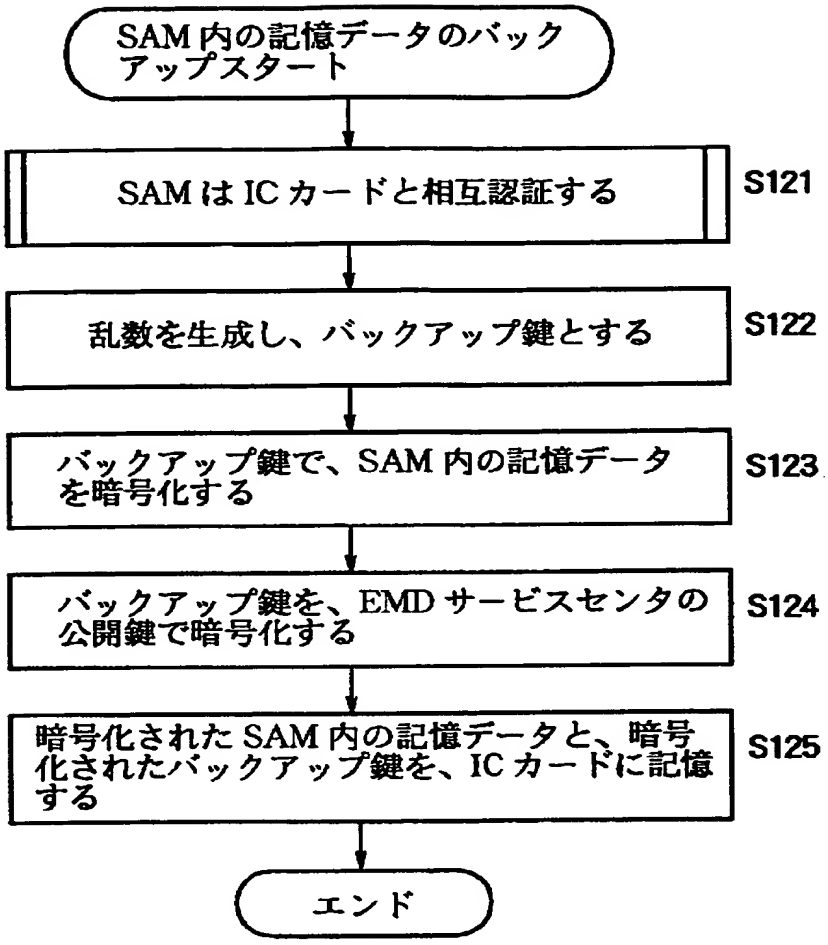
【図３７】


SAMの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAMの名前(ID)
SAMの公開鍵Kpu
他のSAMに従属するかを示すパラメータ
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAMの名前(ID)
SAMの公開鍵Kpu
他のSAMに従属するかを示すパラメータ

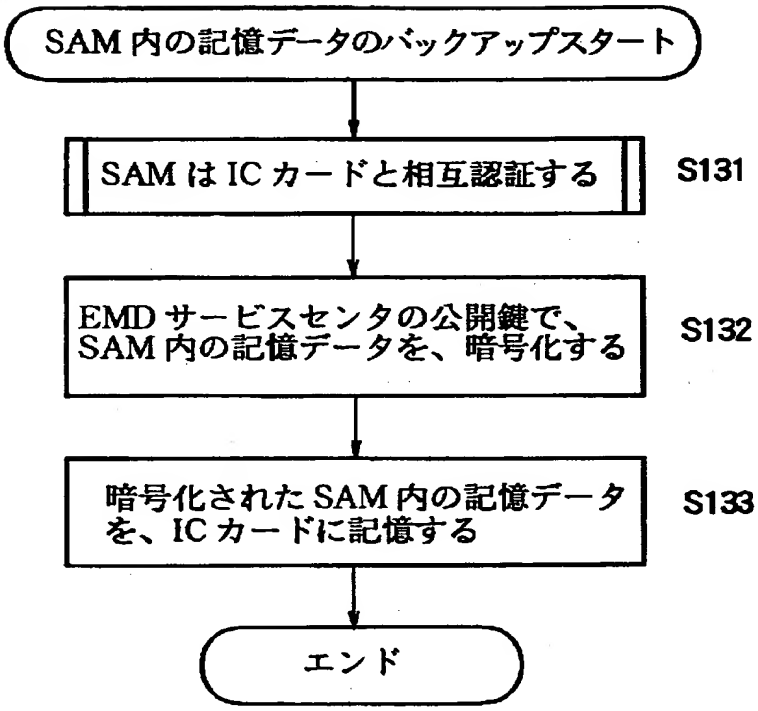
【図３８】

	SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
	0000000000000001h	1	0000	0	xxxxxxxxx
	0000000000000002h	1	1010	1	xxxxxxxxx
	0000000000000003h	1	1100	1	xxxxxxxxx
	000000000000000Ah	0	0000	1	xxxxxxxxx

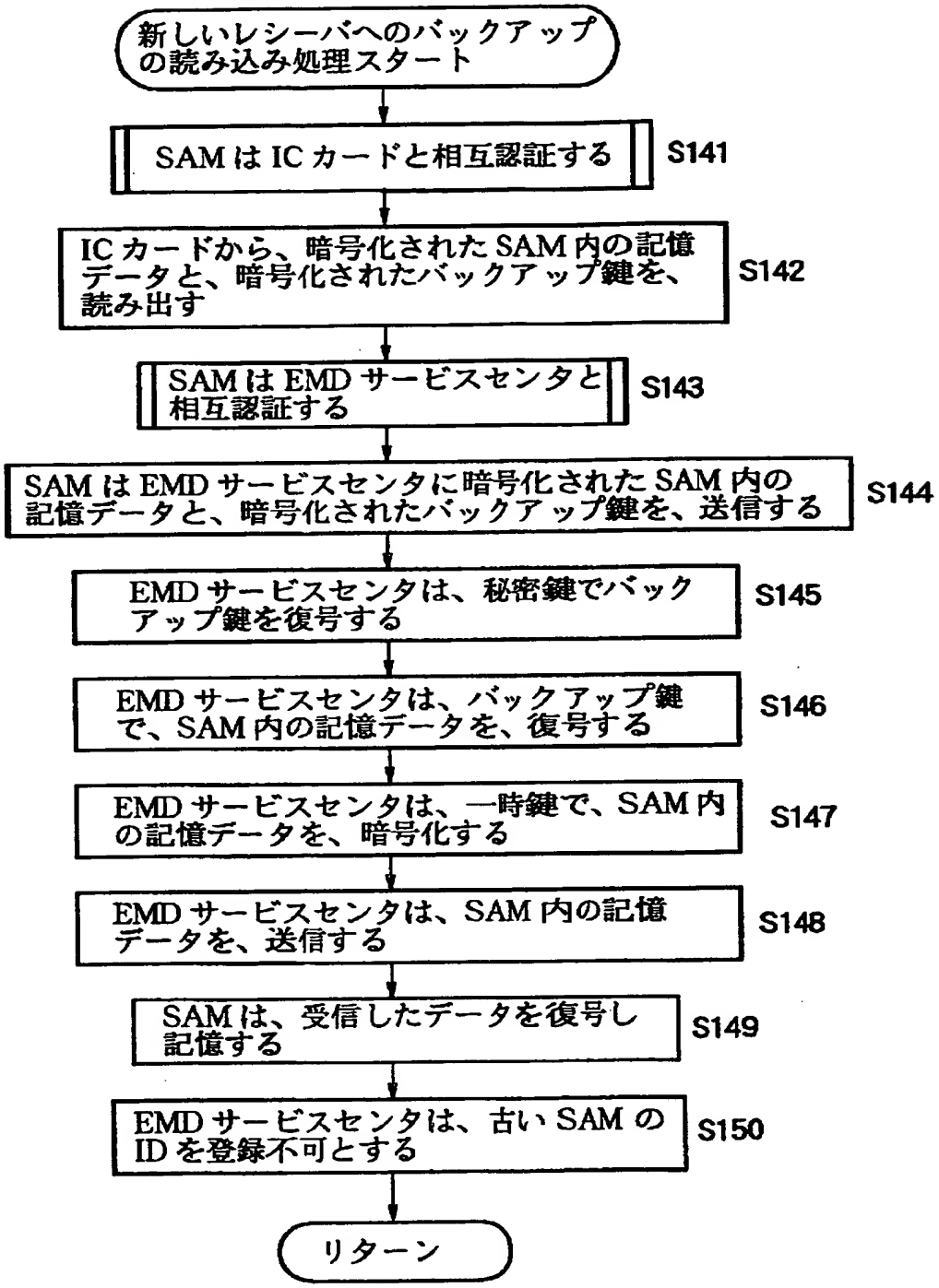
【図３９】


SAM内の記憶データのバックアップスタート
SAMはICカードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM内の記憶データを暗号化する
S123
バックアップ鍵を、EMDサービスセンタの公開鍵で暗号化する
S124
暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、ICカードに記憶する
S125
エンド

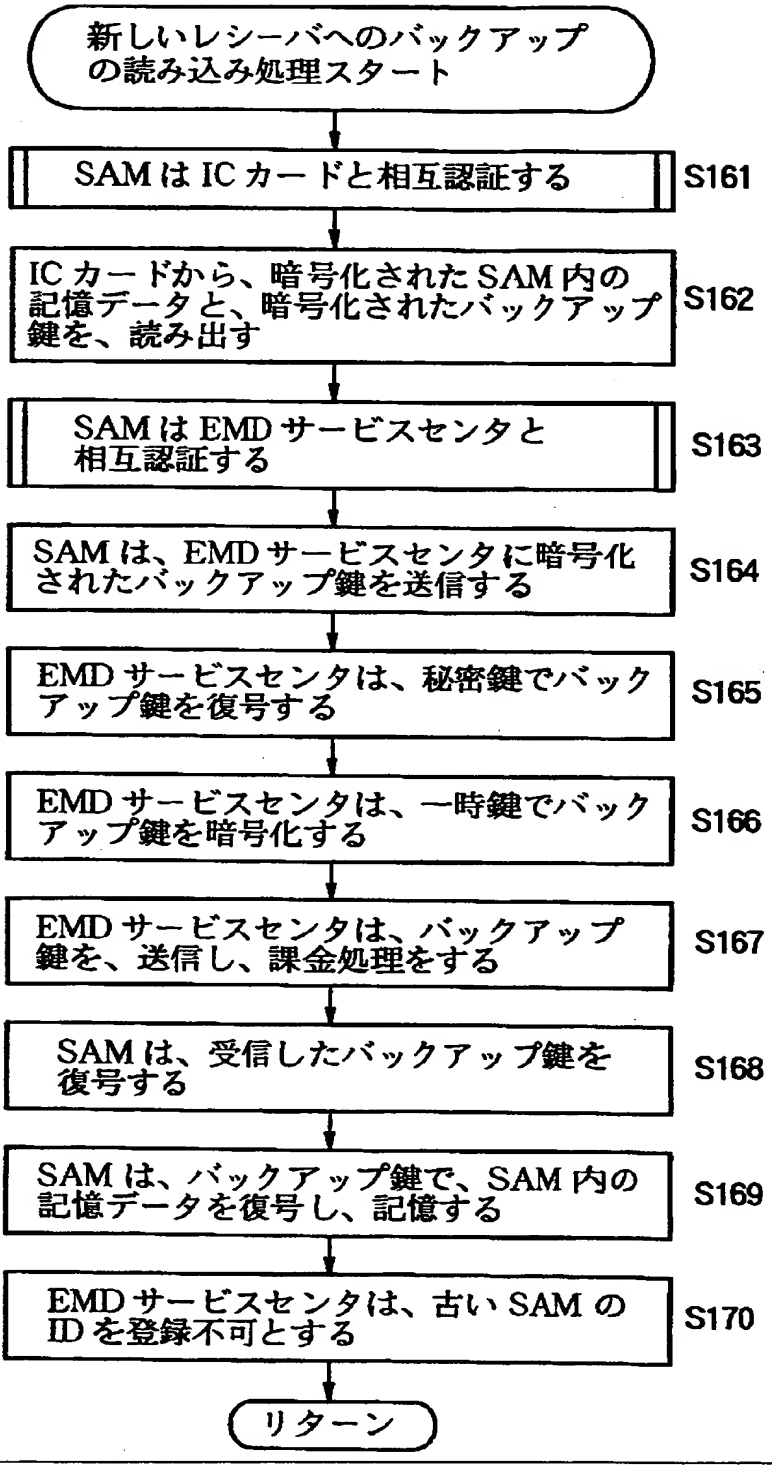
【図４０】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S131
EMD サービスセンタの公開鍵で、SAM 内の記憶データを、暗号化する
S132
暗号化された SAM 内の記憶データを、IC カードに記憶する
S133
エンド

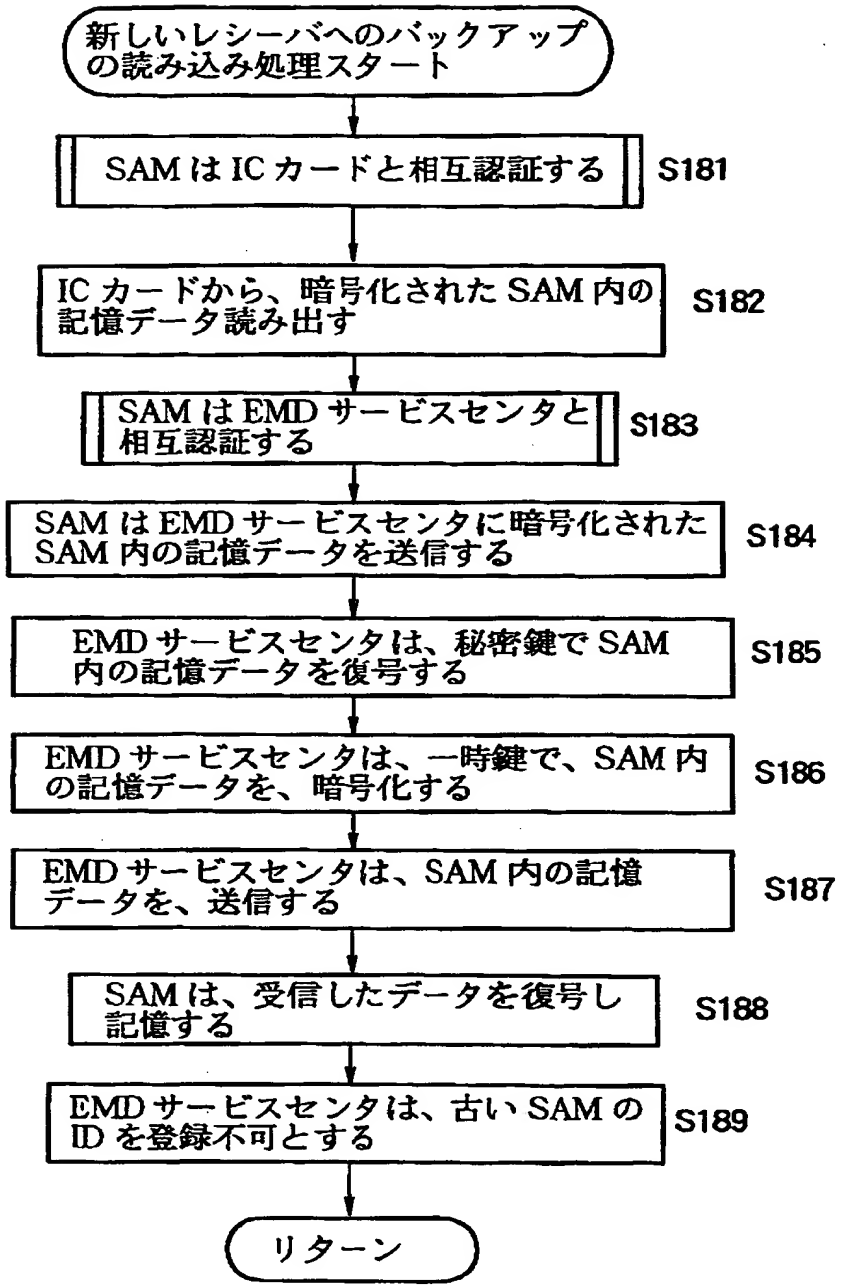
【図４１】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S141
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S142
SAMはEMDサービスセンタと相互認証する
S143
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、送信する
S144
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S145
EMDサービスセンタは、バックアップ鍵で、SAM内の記憶データを、復号する
S146
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S147
EMDサービスセンタは、SAM内の記憶データを、送信する
S148
SAMは、受信したデータを復号し記憶する
S149
EMDサービスセンタは、古いSAMのIDを登録不可とする
S150
リターン

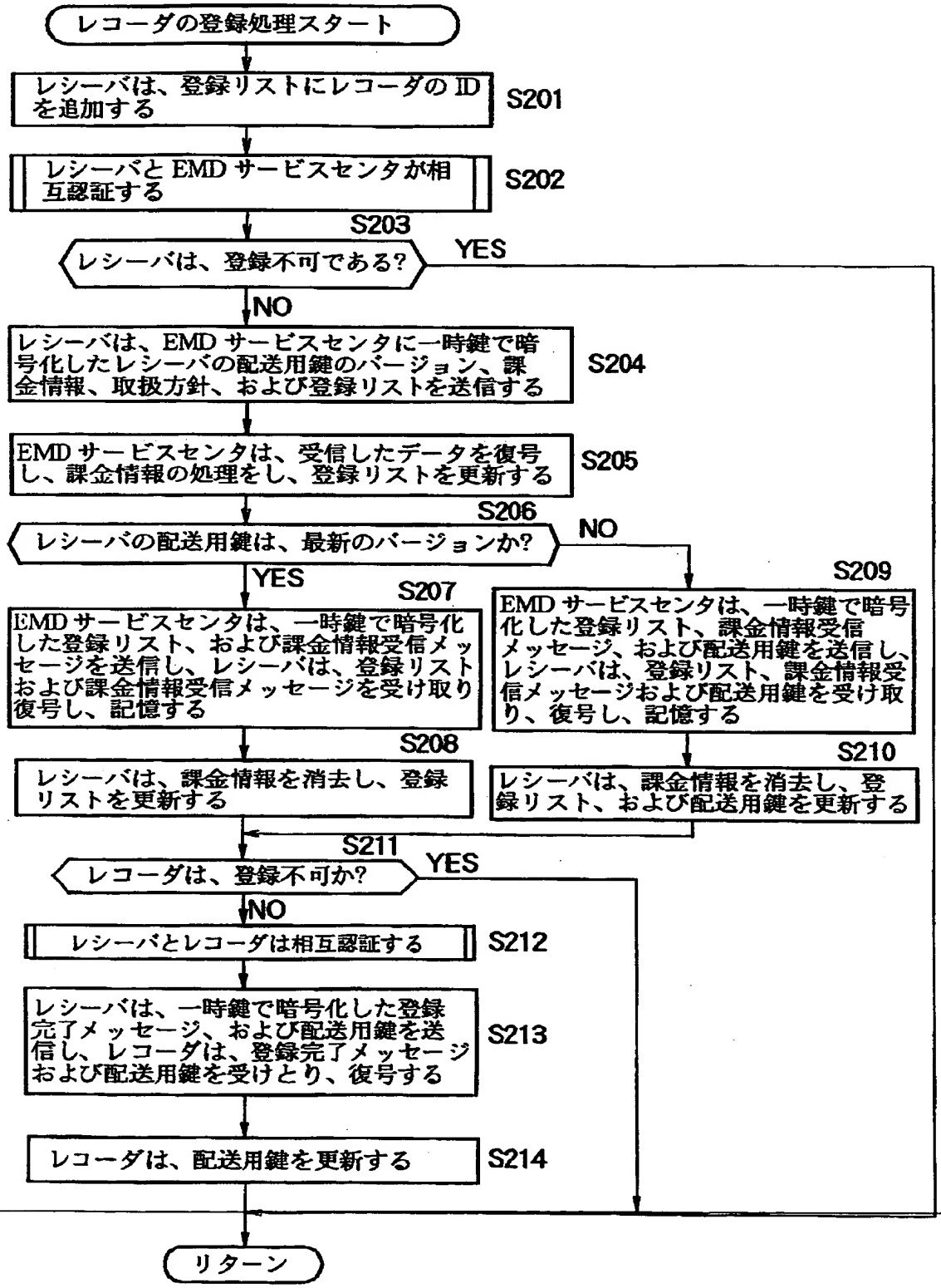
【図４２】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S161
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S162
SAMはEMDサービスセンタと相互認証する
S163
SAMは、EMDサービスセンタに暗号化されたバックアップ鍵を送信する
S164
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S165
EMDサービスセンタは、一時鍵でバックアップ鍵を暗号化する
S166
EMDサービスセンタは、バックアップ鍵を、送信し、課金処理をする
S167
SAMは、受信したバックアップ鍵を復号する
S168
SAMは、バックアップ鍵で、SAM内の記憶データを復号し、記憶する
S169
EMDサービスセンタは、古いSAMのIDを登録不可とする
S170
リターン

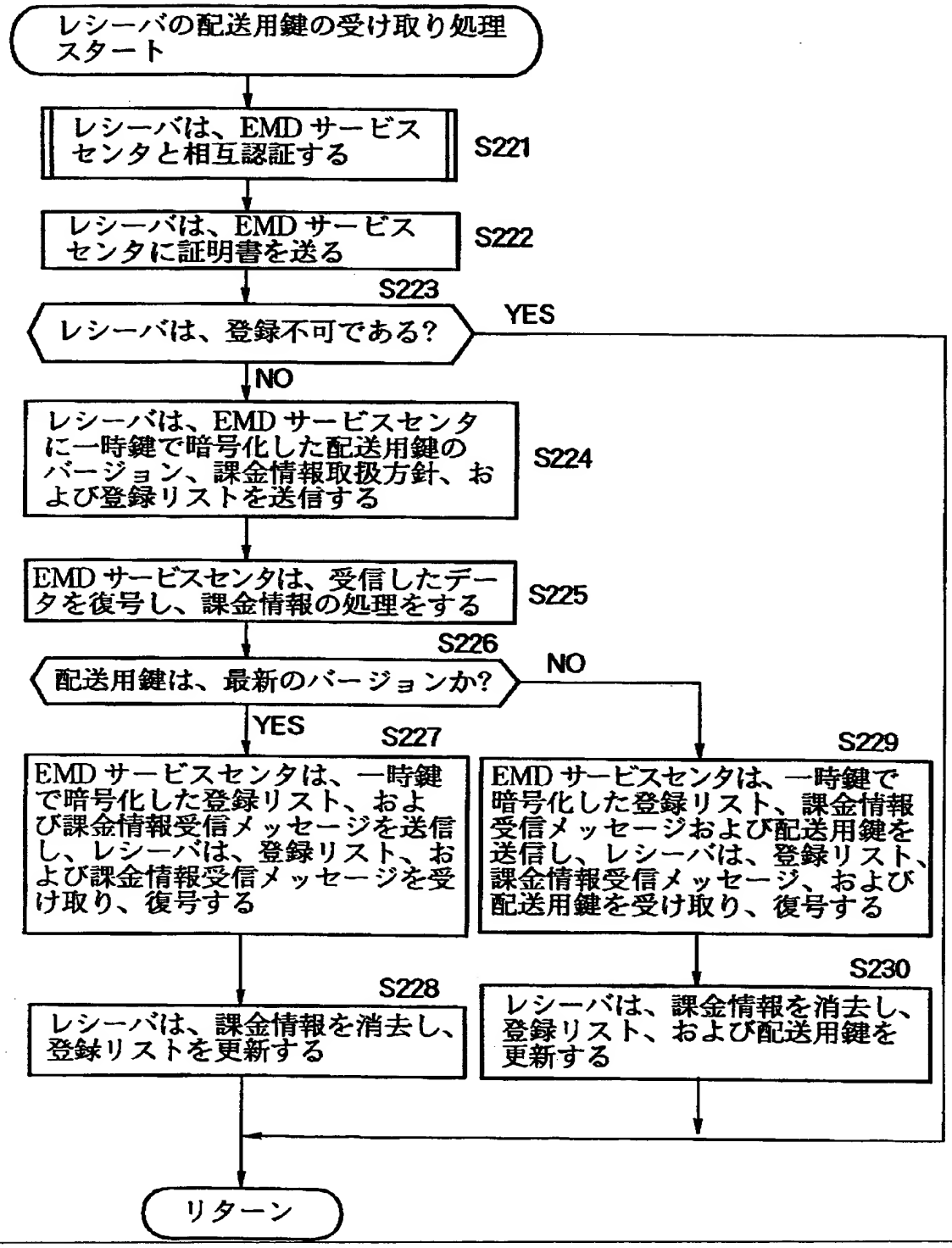
【図４３】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S181
ICカードから、暗号化されたSAM内の記憶データ読み出す
S182
SAMはEMDサービスセンタと相互認証する
S183
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データを送信する
S184
EMDサービスセンタは、秘密鍵でSAM内の記憶データを復号する
S185
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S186
EMDサービスセンタは、SAM内の記憶データを、送信する
S187
SAMは、受信したデータを復号し記憶する
S188
EMDサービスセンタは、古いSAMのIDを登録不可とする
S189
リターン

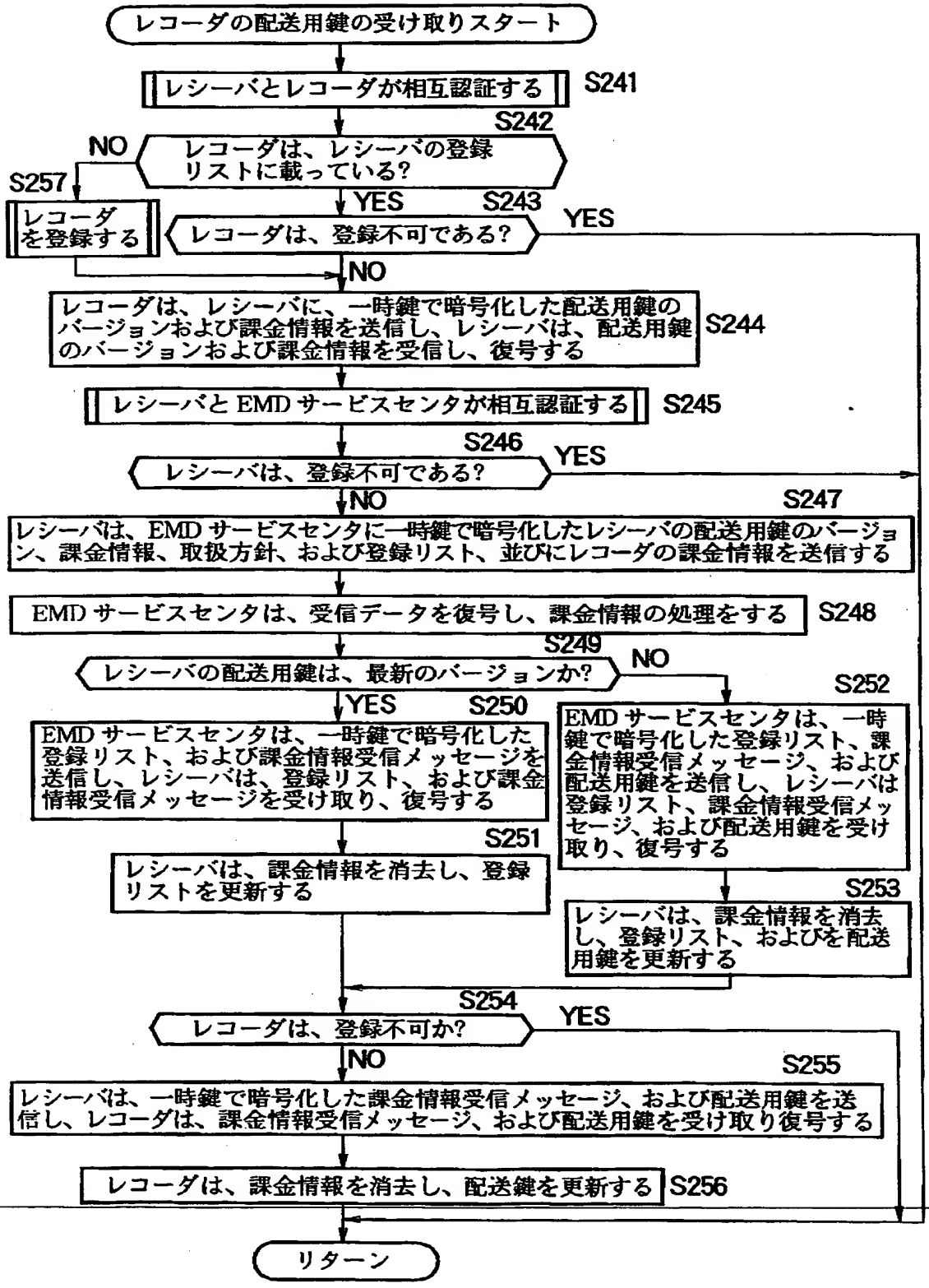
【図４４】


レコーダの登録処理スタート
レシーバは、登録リストにレコーダのIDを追加する
S201
レシーバとEMDサービスセンタが相互認証する
S202
S203
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リストを送信する
S204
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をし、登録リストを更新する
S205
S206
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S207
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リストおよび課金情報受信メッセージを受け取り復号し、記憶する
S209
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージおよび配送用鍵を受け取り、復号し、記憶する
S208
レシーバは、課金情報を消去し、登録リストを更新する
S210
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
S211
レコーダは、登録不可か?
YES
NO
レシーバとレコーダは相互認証する
S212
レシーバは、一時鍵で暗号化した登録完了メッセージ、および配送用鍵を送信し、レコーダは、登録完了メッセージおよび配送用鍵を受けとり、復号する
S213
レコーダは、配送用鍵を更新する
S214
リターン

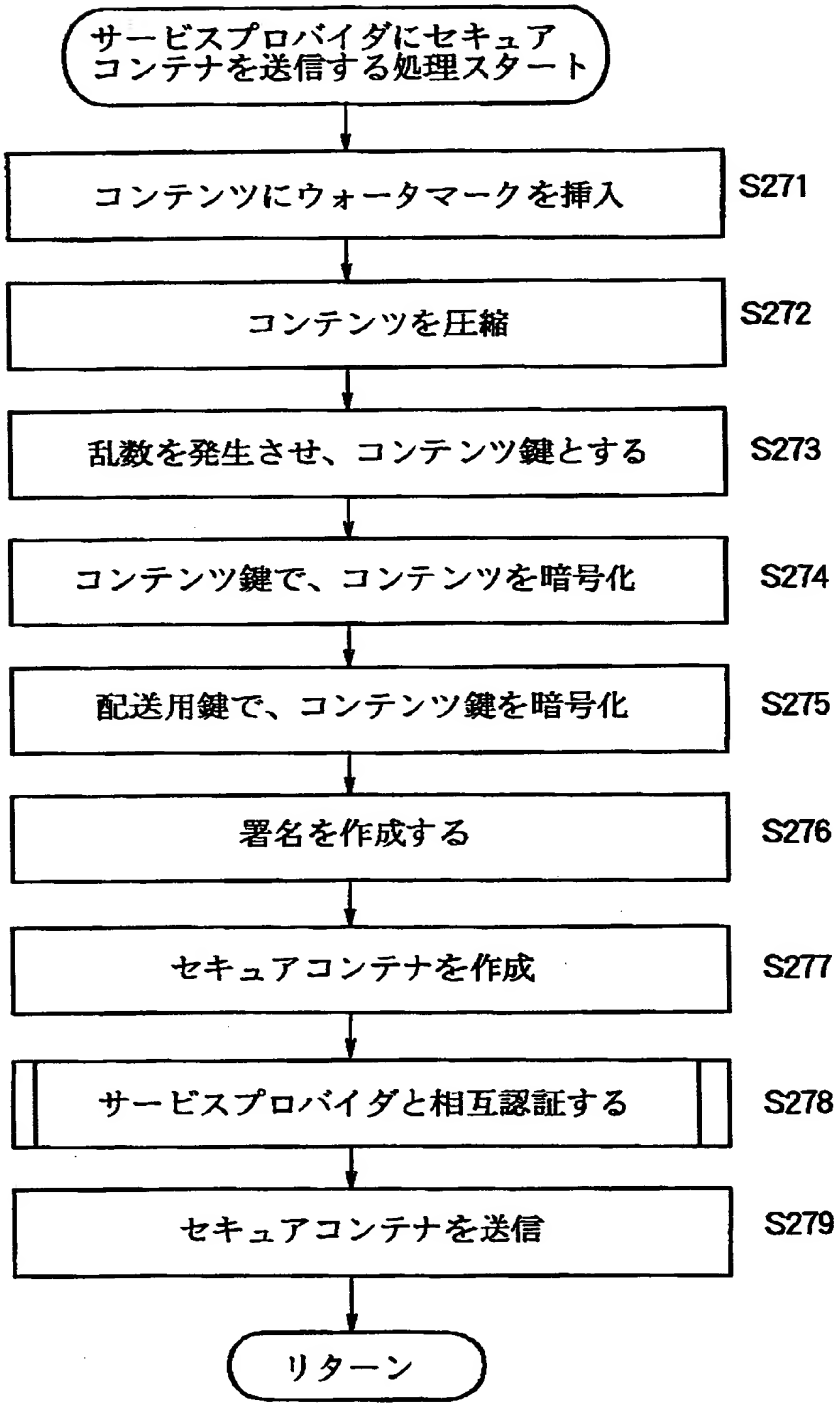
【図４５】


レシーバの配送用鍵の受け取り処理スタート
レシーバは、EMDサービスセンタと相互認証する
S221
レシーバは、EMDサービスセンタに証明書を送る
S222
S223
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化した配送用鍵のバージョン、課金情報取扱方針、および登録リストを送信する
S224
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をする
S225
S226
配送用鍵は、最新のバージョンか?
NO
YES
S227
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S229
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージおよび配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S228
レシーバは、課金情報を消去し、登録リストを更新する
S230
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
リターン

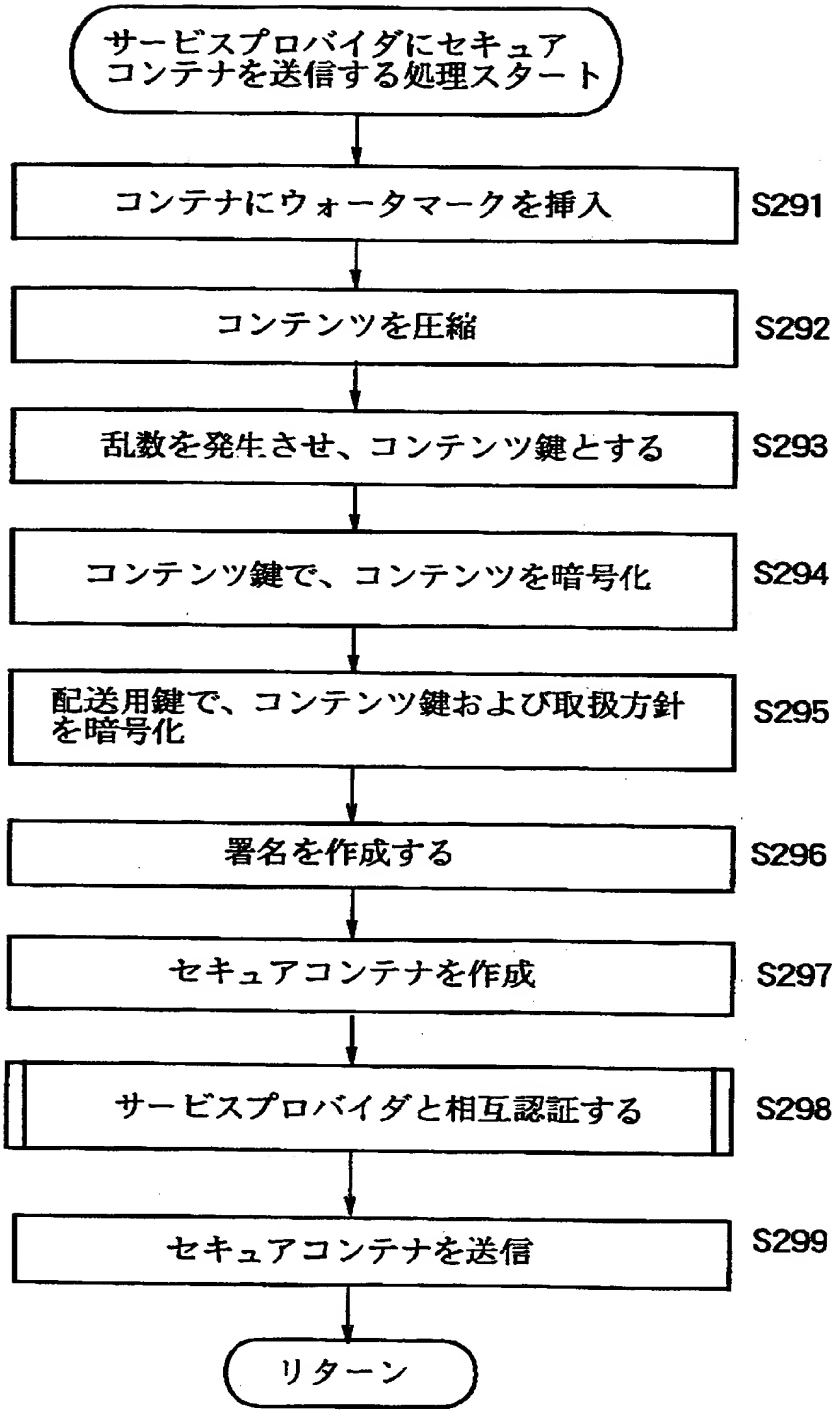
【図４６】


レコーダの配送用鍵の受け取りスタート
レシーバとレコーダが相互認証する
S241
S242
レコーダは、レシーバの登録リストに載っている?
NO
S257
レコーダを登録する
YES
S243
レコーダは、登録不可である?
YES
NO
レコーダは、レシーバに、一時鍵で暗号化した配送用鍵のバージョンおよび課金情報を送信し、レシーバは、配送用鍵のバージョンおよび課金情報を受信し、復号する
S244
レシーバとEMDサービスセンタが相互認証する
S245
S246
レシーバは、登録不可である?
YES
NO
S247
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リスト、並びにレコーダの課金情報を送信する
EMDサービスセンタは、受信データを復号し、課金情報の処理をする
S248
S249
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S250
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S252
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S251
レシーバは、課金情報を消去し、登録リストを更新する
S253
レシーバは、課金情報を消去し、登録リスト、およびを配送用鍵を更新する
S254
レコーダは、登録不可か?
YES
NO
S255
レシーバは、一時鍵で暗号化した課金情報受信メッセージ、および配送用鍵を送信し、レコーダは、課金情報受信メッセージ、および配送用鍵を受け取り復号する
レコーダは、課金情報を消去し、配送鍵を更新する
S256
リターン

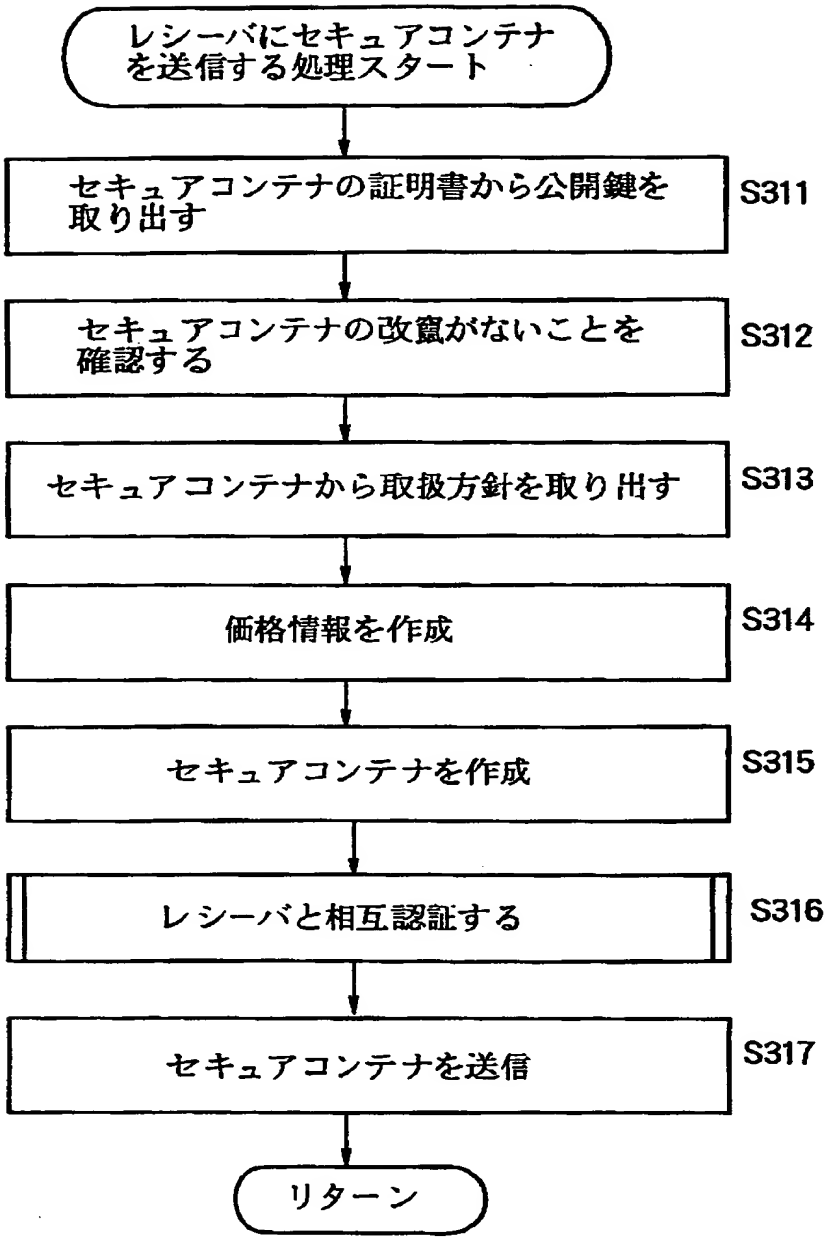
【図４７】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテンツにウォータマークを挿入
S271
コンテンツを圧縮
S272
乱数を発生させ、コンテンツ鍵とする
S273
コンテンツ鍵で、コンテンツを暗号化
S274
配送用鍵で、コンテンツ鍵を暗号化
S275
署名を作成する
S276
セキュアコンテナを作成
S277
サービスプロバイダと相互認証する
S278
セキュアコンテナを送信
S279
リターン

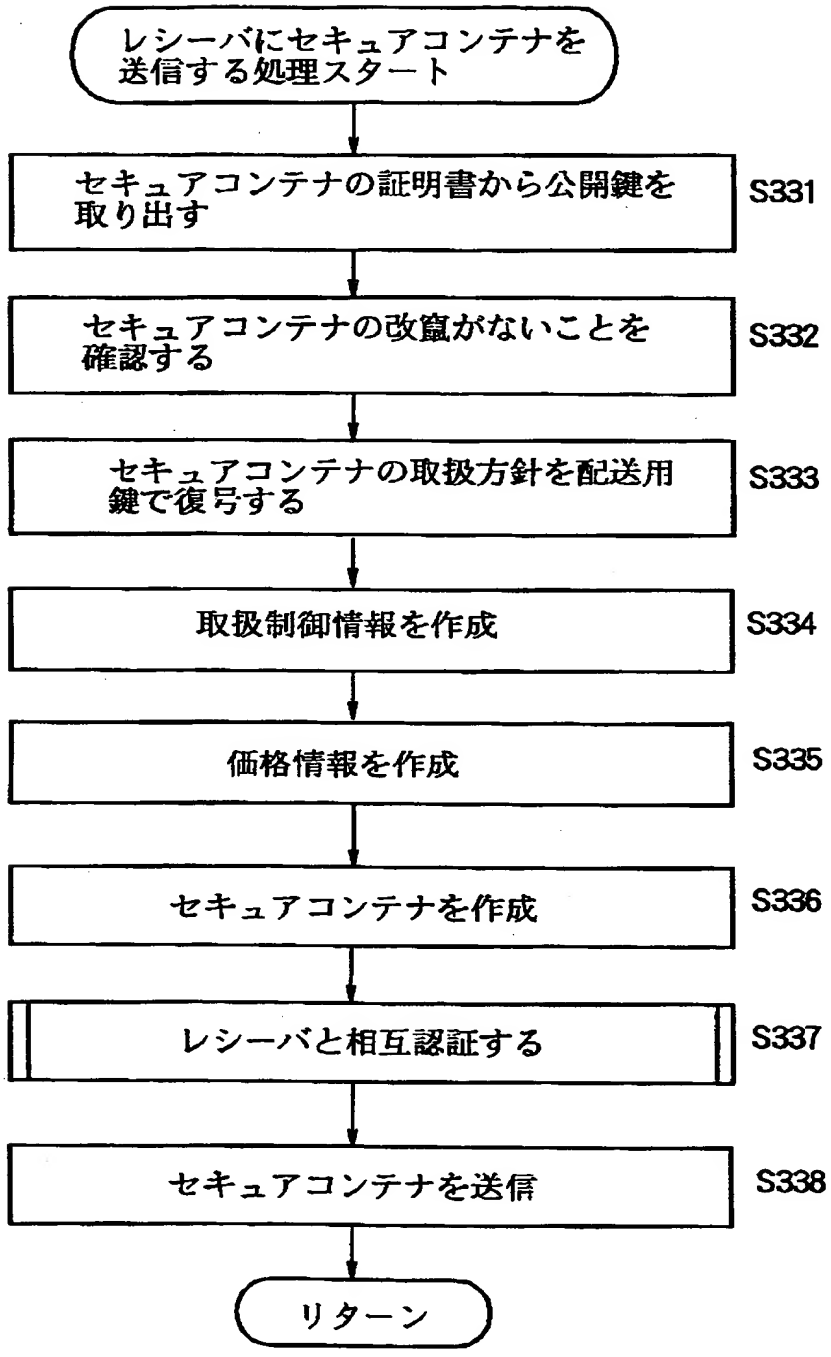
【図４８】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテナにウォータマークを挿入
S291
コンテンツを圧縮
S292
乱数を発生させ、コンテンツ鍵とする
S293
コンテンツ鍵で、コンテンツを暗号化
S294
配送用鍵で、コンテンツ鍵および取扱方針を暗号化
S295
署名を作成する
S296
セキュアコンテナを作成
S297
サービスプロバイダと相互認証する
S298
セキュアコンテナを送信
S299
リターン

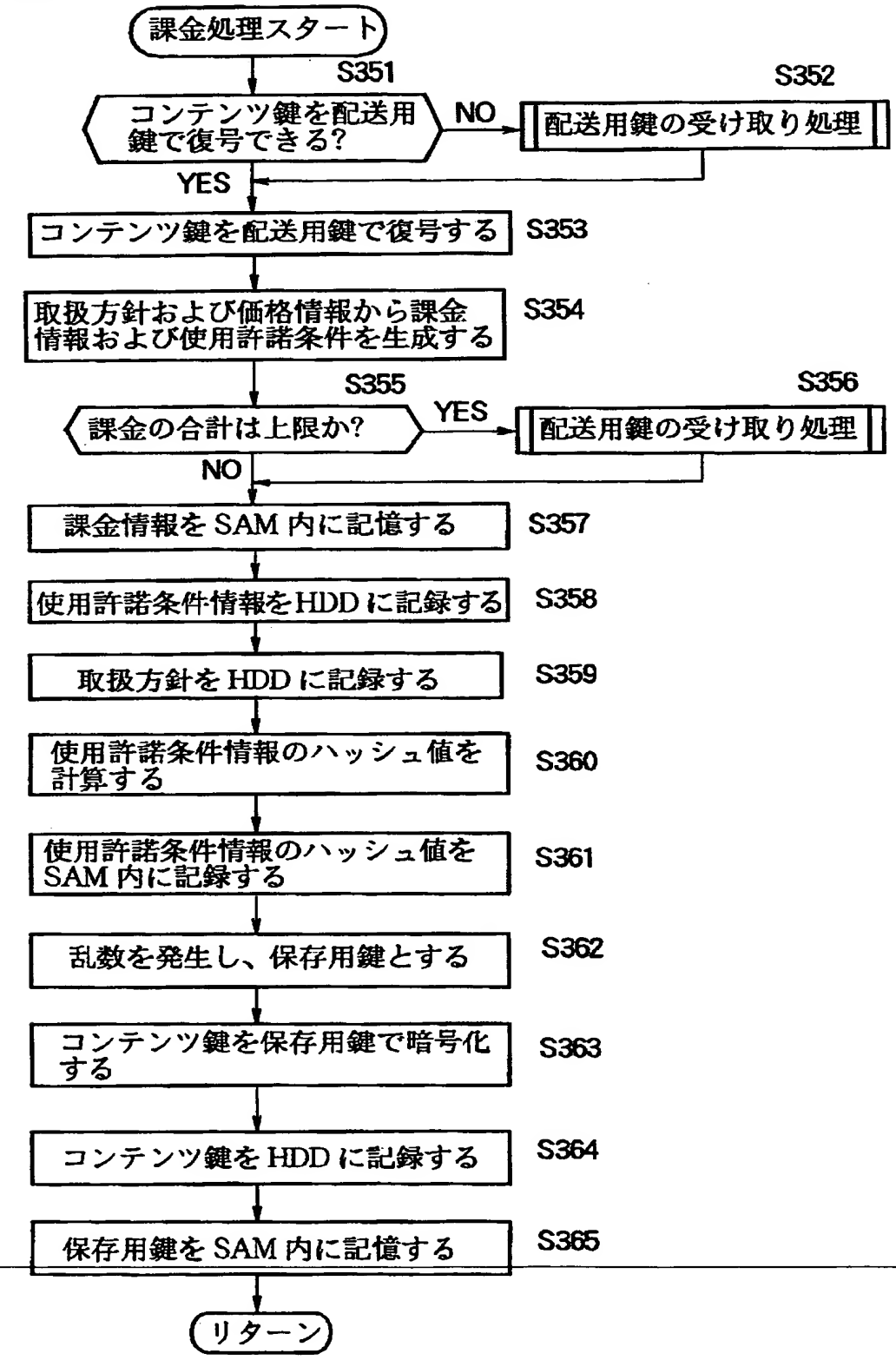
【図４９】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S311
セキュアコンテナの改竄がないことを確認する
S312
セキュアコンテナから取扱方針を取り出す
S313
価格情報を作成
S314
セキュアコンテナを作成
S315
レシーバと相互認証する
S316
セキュアコンテナを送信
S317
リターン

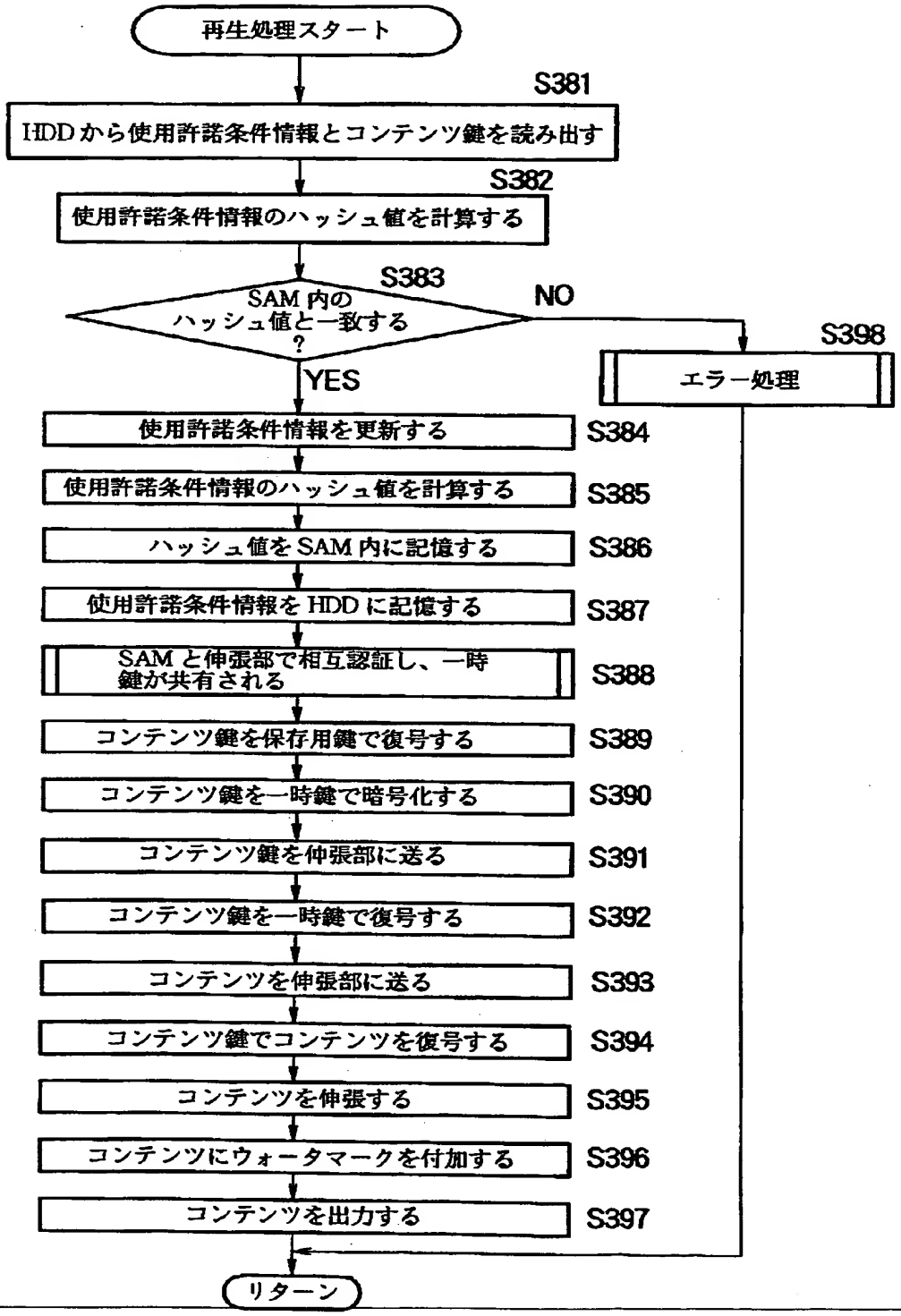
【図５０】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S331
セキュアコンテナの改竄がないことを確認する
S332
セキュアコンテナの取扱方針を配送用鍵で復号する
S333
取扱制御情報を作成
S334
価格情報を作成
S335
セキュアコンテナを作成
S336
レシーバと相互認証する
S337
セキュアコンテナを送信
S338
リターン

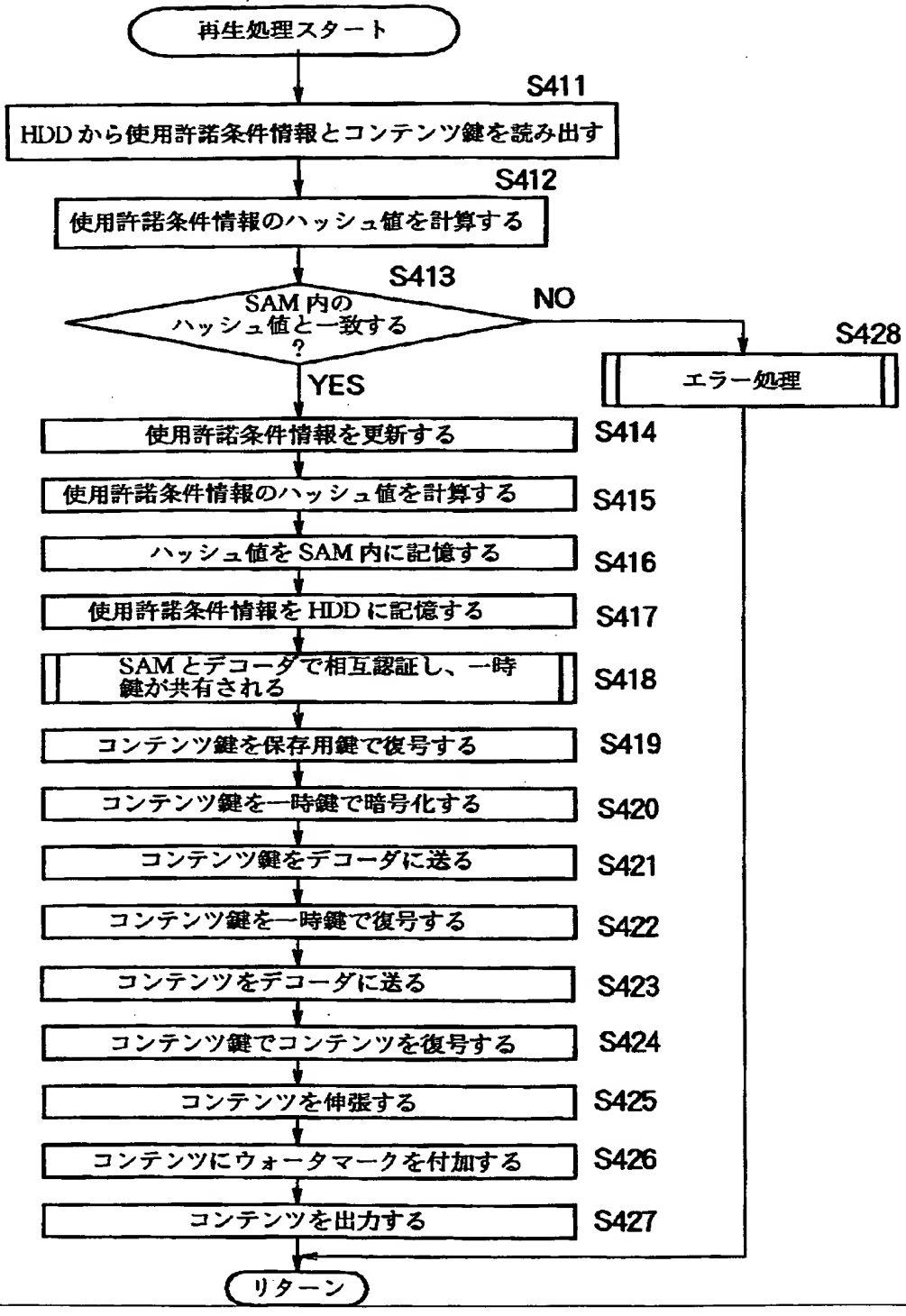
【図５１】


課金処理スタート
S351
コンテンツ鍵を配送用鍵で復号できる?
NO
S352
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S353
取扱方針および価格情報から課金情報および使用許諾条件を生成する
S354
S355
課金の合計は上限か?
YES
S356
配送用鍵の受け取り処理
NO
課金情報をSAM内に記憶する
S357
使用許諾条件情報をHDDに記録する
S358
取扱方針をHDDに記録する
S359
使用許諾条件情報のハッシュ値を計算する
S360
使用許諾条件情報のハッシュ値をSAM内に記録する
S361
乱数を発生し、保存用鍵とする
S362
コンテンツ鍵を保存用鍵で暗号化する
S363
コンテンツ鍵をHDDに記録する
S364
保存用鍵をSAM内に記憶する
S365
リターン

【図５２】


再生処理スタート
S381
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S382
使用許諾条件情報のハッシュ値を計算する
S383
SAM内のハッシュ値と一致する？
NO
S398
エラー処理
YES
使用許諾条件情報を更新する
S384
使用許諾条件情報のハッシュ値を計算する
S385
ハッシュ値をSAM内に記憶する
S386
使用許諾条件情報をHDDに記憶する
S387
SAMと伸張部で相互認証し、一時鍵が共有される
S388
コンテンツ鍵を保存用鍵で復号する
S389
コンテンツ鍵を一時鍵で暗号化する
S390
コンテンツ鍵を伸張部に送る
S391
コンテンツ鍵を一時鍵で復号する
S392
コンテンツを伸張部に送る
S393
コンテンツ鍵でコンテンツを復号する
S394
コンテンツを伸張する
S395
コンテンツにウォータマークを付加する
S396
コンテンツを出力する
S397
リターン

【図５３】


再生処理スタート
S411
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S412
使用許諾条件情報のハッシュ値を計算する
S413
SAM内のハッシュ値と一致する？
NO
S428
エラー処理
YES
使用許諾条件情報を更新する
S414
使用許諾条件情報のハッシュ値を計算する
S415
ハッシュ値をSAM内に記憶する
S416
使用許諾条件情報をHDDに記憶する
S417
SAMとデコーダで相互認証し、一時鍵が共有される
S418
コンテンツ鍵を保存用鍵で復号する
S419
コンテンツ鍵を一時鍵で暗号化する
S420
コンテンツ鍵をデコーダに送る
S421
コンテンツ鍵を一時鍵で復号する
S422
コンテンツをデコーダに送る
S423
コンテンツ鍵でコンテンツを復号する
S424
コンテンツを伸張する
S425
コンテンツにウォータマークを付加する
S426
コンテンツを出力する
S427
リターン

【書類名】　　要約書

【要約】

【課題】　不正に対する安全性を保持したまま、必要な情報を外部に記憶できるようにする。

【解決手段】　相互認証モジュール７１は、装着された外部記憶媒体と相互認証し、暗号化ユニット９３は、所定の鍵で所定の情報を暗号化する。

【選択図】　　図１０

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100082131
【住所又は居所】　東京都新宿区西新宿７丁目５番８号　ＧＯＷＡ西新宿ビル６Ｆ　稲本国際特許事務所
【氏名又は名称】　稲本　義雄

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社